Management Software

AT-S63

Web Browser Interface User's Guide

AT-9400 Series Layer 2+ Gigabit Ethernet Switches

Version 1.2.0

PN 613-50592-00 Rev C

Allied Telesyn

Copyright © 2005 Allied Telesyn, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface 17
How This Guide is Organized 18
Document Conventions 19
Where to Find Web-based Guides 20
Contacting Allied Telesyn 21
Online Support 21
Email and Telephone Support 21
Returning Products 21
Sales or Corporate Information 21
Management Software Updates 21
New Features in AT-S63 Version 1.2.0 22

Section I: Basic Operations 25

Chapter 1: Starting a Web Browser Management Session 27
Establishing a Remote Connection to Use the Web Browser Interface 28
Web Browser Tools 31
Saving Your Parameter Changes 32
Quitting a Web Browser Management Session 33
Ports 23R and 24R on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series Switches 34
Web Browser Interface Restrictions 35

Chapter 2: Basic Switch Parameters 37
Configuring an IP Address and Switch Name 38
Activating the BOOTP or DHCP Client Software 41
Displaying System Information 42
Configuring the Manager and Operator Passwords 44
Rebooting a Switch 46
Setting the System Date and Time 47
Pinging a Remote System 50
Returning the AT-S63 Management Software to the Factory Default Values 52

Chapter 3: Enhanced Stacking 55
Setting a Switch's Enhanced Stacking Status 56
Selecting a Switch in an Enhanced Stack 58
Returning to the Master Switch 61
Displaying the Enhanced Stacking Status 62

Chapter 4: SNMPv1 and SNMPv2c 63
Enabling or Disabling SNMP Management 64
Creating a New SNMPv1 and SNMPv2c Community 66
Modifying an SNMPv1 and SNMPv2c Community 69
Deleting an SNMPv1 and SNMPv2c Community 72
Displaying the SNMPv1 and SNMPv2c Communities 73

Chapter 5: Port Parameters 77
Configuring Port Parameters 78
Displaying Port Status 85
Displaying Port Statistics 89
Resetting a Port to the Default Settings 92

Chapter 6: MAC Address Table 93
Adding Static Unicast and Multicast MAC Addresses 94
Deleting Unicast and Multicast MAC Addresses 96
Deleting All Dynamic MAC Addresses 97
Displaying the MAC Address Tables 98
Changing the Aging Time 101

Chapter 7: Static Port Trunks 103
Creating a Static Port Trunk 104
Modifying a Static Port Trunk 107
Deleting a Port Trunk 109
Displaying the Port Trunks 110

Chapter 8: Port Mirroring 113
Creating a Port Mirror 114
Modifying a Port Mirror 117
Disabling a Port Mirror 118
Deleting a Port Mirror 119
Displaying the Port Mirror 120

Section II: Advanced Operations 123

Chapter 9: File System 125
Listing the Files in Flash Memory or on a Compact Flash Card 126
Selecting an Active Boot Configuration File 130

Chapter 10: File Downloads and Uploads 133
Downloading a File 134
Guidelines 134
Uploading a File 139

Chapter 11: Event Logs and Syslog Servers 141
Working with the Event Logs 142
Enabling or Disabling the Event Logs 142
Displaying Events 144
Clearing an Event Log 150
Saving an Event Log to a File 150
Working with Log Outputs 152
Configuring a Log Output Definition 152
Viewing a Log Output Definition 154
Modifying a Log Output Definition 156
Deleting a Log Output Definition 158

Chapter 12: Classifiers 159
Configuring a Classifier 160
Modifying a Classifier 166
Deleting a Classifier 168
Displaying the Classifiers 169

Chapter 13: Access Control Lists 171
Configuring an Access Control List 172
Modifying an Access Control List 175
Deleting an Access Control List 177
Displaying the Access Control Lists 178

Chapter 14: Class of Service 181
Configuring CoS 182
Mapping CoS Priorities to Egress Queues 184
Configuring Egress Scheduling 186
Displaying the CoS Settings 188
Displaying the QoS Schedule 190

Chapter 15: Quality of Service 191
Managing Flow Groups 192
Configuring Flow Groups 192
Modifying a Flow Group 194
Deleting a Flow Group 195
Displaying Flow Groups 195
Managing Traffic Classes 198
Configuring Traffic Classes 198
Modifying a Traffic Class 200
Deleting a Traffic Class 202
Displaying the Traffic Classes 202
Managing Policies 206
Configuring a Policy 206
Modifying a Policy 208
Deleting a Policy 210
Displaying Policies 210

Chapter 16: Denial of Service Defense 213
Configuring Denial of Service Defense 214
Displaying the DoS Settings 217

Chapter 17: IGMP Snooping 219
Configuring IGMP Snooping 220
Displaying a List of Host Nodes 223
Displaying a List of Multicast Routers 226

Section III: SNMPv3 229

Chapter 18: SNMPv3 231
Configuring the SNMPv3 Protocol 232
Enabling or Disabling SNMP Management 233
Configuring the SNMPv3 User Table 236
Creating a User Table Entry 236
Deleting a User Table Entry 239
Modifying a User Table Entry 240
Configuring the SNMPv3 View Table 244
Creating a View Table Entry 244
Deleting a View Table Entry 247
Modifying a View Table Entry 247
Configuring the SNMPv3 Access Table 250
Creating an Access Table 250
Deleting an Access Table Entry 253
Modifying an Access Table Entry 254

Configuring the SNMPv3 SecurityToGroup Table 257
Creating a SecurityToGroup Table Entry 257
Deleting a SecurityToGroup Table Entry 260
Modifying a SecurityToGroup Table Entry 260
Configuring the SNMPv3 Notify Table 263
Creating a Notify Table Entry 263
Deleting a Notify Table Entry 265
Modifying a Notify Table Entry 266
Configuring the SNMPv3 Target Address Table 268
Creating a Target Address Table Entry 268
Deleting a Target Address Table Entry 271
Modifying Target Address Table Entry 272
Configuring the SNMPv3 Target Parameters Table 275
Creating a Target Parameters Table Entry 275
Deleting a Target Parameters Table Entry 278
Modifying a Target Parameters Table Entry 279
Configuring the SNMPv3 Community Table 282
Creating an SNMPv3 Community Table Entry 282
Deleting an SNMPv3 Community Table Entry 285
Modifying an SNMPv3 Community Table Entry 285
Displaying SNMPv3 Tables 288
Displaying User Table Entries 288
Displaying View Table Entries 290
Displaying Access Table Entries 291
Displaying SecurityToGroup Table Entries 292
Displaying Notify Table Entries 293
Displaying Target Address Table Entries 294
Displaying Target Parameters Table Entries 295
Displaying SNMPv3 Community Table Entries 296

Section IV: Spanning Tree Protocols 299

Chapter 19: Spanning Tree and Rapid Spanning Tree Protocols 301
Enabling or Disabling a Spanning Tree Protocol 302
Configuring STP 304
Displaying the STP Settings 308
Resetting STP to the Default Settings 311
Configuring RSTP 312
Resetting RSTP to the Default Settings 316
Displaying RSTP Settings 316

Chapter 20: Multiple Spanning Tree Protocol 319
Enabling MSTP 320
Configuring MSTP 322
Configuring MSTP Parameters 322
Configuring the CIST Priority 325
Creating, Deleting, or Modifying MSTI IDs 326
Creating an MSTI ID 326
Deleting an MSTI ID 327
Modifying an MSTI ID 328
Adding, Removing, or Modifying VLAN Associations to MSTIs 330
Adding a VLAN Association 330
Removing a VLAN Association 330
Modifying a VLAN Association 331
Configuring MSTP Port Parameters 333

Displaying the MSTP Port Configuration 337
Displaying the MSTP Port Status 340
Resetting MSTP to the Default Settings 342

Section V: Virtual LANs 343

Chapter 21: Port-based and Tagged VLANs 345
Creating a New Port-Based or Tagged VLAN 346
Modifying a VLAN 350
Deleting a VLAN 352
Selecting a VLAN Mode 353
Displaying VLANs 355
Specifying a Management VLAN 357

Chapter 22: GARP VLAN Registration Protocol 359
Configuring GVRP 360
Enabling or Disabling GVRP on a Port 362
Displaying the GVRP Configuration 363
Displaying the GVRP Port Configuration 365
Displaying the GVRP Database 366
Displaying the GVRP State Machine 367
Displaying the GVRP Counters 370
Displaying the GIP Connected Ports Ring 373

Chapter 23: Protected Ports VLANs 375
Creating a New Protected Ports VLAN 376
Modifying a Protected Ports VLAN 381
Deleting a Protected Ports VLAN 385
Displaying a Protected Ports VLAN 386

Section VI: Port Security 389

Chapter 24: MAC Address-based Port Security 391
Configuring Port Security 392
Displaying the Port Security Level 395

Chapter 25: 802.1x Port-based Network Access Control 397
Setting Port Roles 398
Enabling or Disabling 802.1x Port-based Network Access Control 400
Configuring Authenticator Port Parameters 401
Configuring Supplicant Port Parameters 405
Displaying the Port-based Network Access Control Parameters 407
    Displaying the Port Status 407
    Displaying the Port Settings 408
RADIUS Accounting 411
    Configuring RADIUS Accounting 411
    Displaying the RADIUS Accounting Settings 412

Section VII: Management Security 415

Chapter 26: Encryption Keys, PKI, and SSL 417
Displaying the Encryption Keys 418
Displaying the PKI Settings and Certificates 420
Displaying the SSL Settings 423

Chapter 27: Secure Shell (SSH) 425
Configuring SSH 426
Displaying the SSH Settings 428

Chapter 28: TACACS+ and RADIUS Protocols 431
Enabling or Disabling TACACS+ or RADIUS 432
Configuring TACACS+ 434
Displaying the TACACS+ Settings 436
Configuring RADIUS 438
Displaying the RADIUS Settings 440

Chapter 29: Management Access Control List 443
Enabling or Disabling the Management ACL 444
Creating an ACE 446
Deleting an ACE 448
Displaying the Management Access Control List 449

Index 451

Figures

Chapter 1: Starting a Web Browser Management Session 27
Figure 1: Entering a Switch's IP Address in the URL Field 28
Figure 2: AT-S63 Login Page 29
Figure 3: Home page 29
Figure 4: Save Config Option in the Configuration Menu 32

Chapter 2: Basic Switch Parameters 37
Figure 5: General Tab (Configuration) 38
Figure 6: General Tab (Monitoring) 42
Figure 7: System Time Tab 48
Figure 8: File System Tab (Monitoring) 50
Figure 9: Ping Client Tab (Monitoring) 51
Figure 10: System Utilities Tab (Configuration) 53

Chapter 3: Enhanced Stacking 55
Figure 11: Enhanced Stacking Tab (Configuration) 57
Figure 12: Stacking Switches Page 59
Figure 13: Enhanced Stacking Tab (Monitoring) 62

Chapter 4: SNMPv1 and SNMPv2c 63
Figure 14: SNMP Tab (Configuration) 64
Figure 15: SNMPv1 & SNMPv2c Communities Tab 66
Figure 16: Add New SNMPv1 & SNMPv2c Community Page 67
Figure 17: Modify SNMPv1 & SNMPv2c Community Page 70
Figure 18: SNMP Tab (Monitoring) 73
Figure 19: SNMPv1 & SNMPv2c Communities Tab (Monitoring) 74

Chapter 5: Port Parameters 77
Figure 20: Port Settings Tab (Configuration) 78
Figure 21: Port Configuration Page 79
Figure 22: Port Settings Tab (Monitoring) 85
Figure 23: Port Status Page 86
Figure 24: Port Statistics Page 89

Chapter 6: MAC Address Table 93
Figure 25: MAC Address Tab (Configuration) 94
Figure 26: Add MAC Address Page 95
Figure 27: MAC Address Tab (Monitoring) 98
Figure 28: View MAC Addresses Page 100

Chapter 7: Static Port Trunks 103
Figure 29: Port Trunking Tab (Configuration) 105
Figure 30: Add New Trunk Page 105
Figure 31: Modify Trunk Page 108
Figure 32: Port Trunking Tab (Monitoring) 110

Chapter 8: Port Mirroring 113
Figure 33: Port Mirroring Tab (Configuration) 114
Figure 34: Modify Mirror Page 115
Figure 35: Example of a Modify Mirror Page 116

Figure 36: Port Mirroring Tab (Monitoring) 120

Chapter 9: File System 125
Figure 37: File System Tab (Configuration) 127
Figure 38: List Files Page 129

Chapter 10: File Downloads and Uploads 133
Figure 39: System Utilities Tab (Configuration) 136

Chapter 11: Event Logs and Syslog Servers 141
Figure 40: Event Log Tab (Configuration) 143
Figure 41: Event Log Tab (Monitoring) 145
Figure 42: Event Log Example Displayed in Normal Mode 148
Figure 43: Event Log Example Displayed in Full Mode 149
Figure 44: Create Event Log Output Page 152
Figure 45: View Event Log Output Page 155
Figure 46: Configure Log Outputs Section 156
Figure 47: Modify Event Log Output Page 156

Chapter 12: Classifiers 159
Figure 48: Classifier Tab (Configuration) 161
Figure 49: Create Classifier Page 162
Figure 50: Create Classifier Page - IP Protocol 162
Figure 51: Modify Classifier Page 166
Figure 52: Classifier Tab (Monitoring) 169
Figure 53: View Classifier Page 170

Chapter 13: Access Control Lists 171
Figure 54: ACL Tab (Configuration) 172
Figure 55: Create ACLs Page 173
Figure 56: Modify ACLs Page 175
Figure 57: ACL Tab (Monitoring) 178
Figure 58: View ACLs Page 179

Chapter 14: Class of Service 181
Figure 59: CoS Tab (Configuration) 182
Figure 60: CoS Setting for Port Page 183
Figure 61: Queuing & Scheduling Tab (Configuration) 184
Figure 62: CoS Tab (Monitoring) 188
Figure 63: CoS Setting for Port Page 189
Figure 64: QoS Scheduling Tab (Monitoring) 190

Chapter 15: Quality of Service 191
Figure 65: Flow Group Tab (Configuration) 192
Figure 66: Create Flow Group Page 193
Figure 67: Modify Flow Group Page 194
Figure 68: Flow Group Tab (Monitoring) 196
Figure 69: View Flow Group Page 197
Figure 70: Traffic Class Tab 198
Figure 71: Create Traffic Class Page 199
Figure 72: Modify Traffic Class Page 201
Figure 73: Traffic Class Tab (Monitoring) 203
Figure 74: View Traffic Class Page 204
Figure 75: Policies Tab (Configuration) 206
Figure 76: Create Policy Page 207
Figure 77: Modify Policy Page 209
Figure 78: Policies Tab (Monitoring) 211
Figure 79: View Policy Page 212

Chapter 16: Denial of Service Defense 213
Figure 80: DoS Tab (Configuration) 214
Figure 81: DoS Configuration for Ports Page 215
Figure 82: DoS Tab (Monitoring) 217
Figure 83: DoS Monitor for Ports Page 218

Chapter 17: IGMP Snooping 219
Figure 84: IGMP Tab (Configuration) 220
Figure 85: IGMP Tab (Monitoring) 223
Figure 86: View Multicast Hosts List Page 224
Figure 87: View Multicast Routers List Page 226
Figure 88: View (Static) Multicast Routers List Page 227

Chapter 18: SNMPv3 231
Figure 89: SNMP Tab (Configuration) 234
Figure 90: SNMPv3 User Table Tab (Configuration) 237
Figure 91: Add New SNMPv3 User Page 237
Figure 92: Modify SNMPv3 User Page 241
Figure 93: SNMPv3 View Table Tab (Configuration) 245
Figure 94: Add New SNMPv3 View Page 245
Figure 95: Modify SNMPv3 View Page 248
Figure 96: SNMPv3 Access Table Tab (Configuration) 250
Figure 97: Add New SNMPv3 Access Page 251
Figure 98: Modify SNMPv3 Access Page 255
Figure 99: SNMPv3 SecurityToGroup Table Tab (Configuration) 258
Figure 100: Add New SNMPv3 SecurityToGroup Page 258
Figure 101: Modify SNMPv3 SecurityToGroup Page 261
Figure 102: SNMPv3 Notify Table Tab (Configuration) 264
Figure 103: Add New SNMPv3 Notify Page 264
Figure 104: Modify SNMPv3 Notify Page 266
Figure 105: SNMPv3 Target Address Table Tab (Configuration) 269
Figure 106: Add New SNMPv3 Target Address Page 269
Figure 107: Modify SNMPv3 Target Address Page 272
Figure 108: SNMPv3 Target Parameters Table Tab (Configuration) 275
Figure 109: Add New SNMPv3 Target Parameters Page 276
Figure 110: Modify SNMPv3 Target Parameter Page 279
Figure 111: SNMPv3 Community Table Tab (Configuration) 283
Figure 112: Add New SNMPv3 Community Page 283
Figure 113: Modify SNMPv3 Community Page 286
Figure 114: SNMP Tab (Monitoring) 289
Figure 115: SNMPv3 User Table Tab (Monitoring) 290
Figure 116: SNMPv3 View Table Tab (Monitoring) 291
Figure 117: SNMPv3 Access Table Tab (Monitoring) 292
Figure 118: SNMPv3 SecurityToGroup Table Tab (Monitoring) 293
Figure 119: SNMPv3 Notify Table Tab (Monitoring) 294
Figure 120: SNMPv3 Target Address Table Tab (Monitoring) 295
Figure 121: SNMPv3 Target Parameters Table Tab (Monitoring) 296
Figure 122: SNMPv3 Community Table Tab (Monitoring) 297

Chapter 19: Spanning Tree and Rapid Spanning Tree Protocols 301
Figure 123: MAC Address Tab (Configuration) 302
Figure 124: Spanning Tree Tab (Configuration) 303
Figure 125: Configure STP Parameters Tab (Configuration) 305
Figure 126: STP Settings - Port(s) Page 307
Figure 127: MAC Address Tab (Monitoring) 309
Figure 128: Spanning Tree Tab (Monitoring) 309
Figure 129: Monitor STP Parameters Tab (Monitoring) 310

Figure 130: STP Settings Page 310
Figure 131: Configure RSTP Parameters Tab (Configuration) 313
Figure 132: RSTP Settings - Port(s) Page 315
Figure 133: Monitor RSTP Parameters Tab (Monitoring) 317
Figure 134: RSTP Settings Page 317

Chapter 20: Multiple Spanning Tree Protocol 319
Figure 135: Spanning Tree Tab (Configuration) 320
Figure 136: Configure MSTP Parameters Tab (Configuration) 323
Figure 137: Add New MSTI Page 326
Figure 138: Modify MSTI Page 328
Figure 139: MSTP Settings - Port(s) Page 333
Figure 140: Monitor MSTP Parameters Tab (Monitoring) 338
Figure 141: MSTP Settings - Port(s) Page 338
Figure 142: MSTP Port Status - Port(s) Page 340

Chapter 21: Port-based and Tagged VLANs 345
Figure 143: VLAN Tab (Configuration) 346
Figure 144: Add New VLAN Page 347
Figure 145: VLAN Tab (Monitoring) 355

Chapter 22: GARP VLAN Registration Protocol 359
Figure 146: GVRP Tab (Configuration) 360
Figure 147: GVRP Port Configuration Page 362
Figure 148: GVRP Tab (Monitoring) 363
Figure 149: GVRP Port Configuration Page 365
Figure 150: GVRP Database Page 366
Figure 151: GVRP State Machine for VLAN Page 367
Figure 152: GVRP Counters Page 370
Figure 153: GIP Connected Ports Ring Page 373

Chapter 23: Protected Ports VLANs 375
Figure 154: Add New VLAN Page 377
Figure 155: Add New Protected VLAN Page 379
Figure 156: Modify Protected VLAN Page 383
Figure 157: View Protected VLAN Page 386

Chapter 24: MAC Address-based Port Security 391
Figure 158: Port Security Tab (Configuration) 392
Figure 159: Security for Ports Page (Configuration) 392
Figure 160: Port Security Tab (Monitoring) 395
Figure 161: Security for Port(s) Page 396

Chapter 25: 802.1x Port-based Network Access Control 397
Figure 162: 802.1x Port Access Tab (Configuration) 398
Figure 163: Port Role Configuration Page 399
Figure 164: Authenticator Parameters Page 402
Figure 165: Supplicant Parameters Page 405
Figure 166: 802.1x Port Access Tab (Monitoring) 407
Figure 167: Port Access Port Status Page 408
Figure 168: Authenticator Port Parameters Page 409
Figure 169: Supplicant Port Parameters Page 410
Figure 170: 802.1x Port Access Tab (Monitoring) 413

Chapter 26: Encryption Keys, PKI, and SSL 417
Figure 171: Keys Tab (Monitoring) 418
Figure 172: PKI Tab (Monitoring) 420
Figure 173: X509 Certificate Details Page 421
Figure 174: SSL Tab (Monitoring) 423

Chapter 27: Secure Shell (SSH) 425
Figure 175: Secure Shell Tab (Configuration) 426
Figure 176: Secure Shell Tab (Monitoring) 428
Chapter 28: TACACS+ and RADIUS Protocols 431
Figure 177: Server-based Authentication Tab (Configuration) 432
Figure 178: TACACS+ Client Configuration Page 434
Figure 179: Server-Based Authentication Tab (Monitoring) 436
Figure 180: TACACS+ Client Configuration Page 437
Figure 181: RADIUS Client Configuration Page 438
Figure 182: RADIUS Client Configuration Page 440
Chapter 29: Management Access Control List 443
Figure 183: Mgmt. ACL Tab (Configuration) 444
Figure 184: Mgmt. ACL Tab (Monitoring) 449

Tables

Table 1: New Features in AT-S63 Version 1.2.0 22
Table 2: AT-S63 Software Modules 147
Table 3: Event Severity Levels 149
Table 4: Default Syslog Facilities 154
Table 5: Default Mappings of IEEE 802.1p Priority Levels to Egress Priority Queues 185
Table 6: Example of Weighted Round Robin Priority 186
Table 7: Bridge Priority Value Increments 306
Table 8: Port Priority Value Increments 307
Table 9: MSTP Auto Update Port Internal Path Costs 334
Table 10: MSTP Auto Update Port Trunk Internal Path Costs 335
Table 11: MSTP Auto External Path Costs 335
Table 12: MSTP Auto External Path Trunk Costs 336
Table 13: GVRP State Machine Parameters 367
Table 14: GVRP Counters 371

Preface

This guide contains instructions on how to configure and maintain an AT-9400 Series Layer 2+ Gigabit Ethernet switch using the web browser interface in the AT-S63 management software.

For instructions on how to manage the switch from the menus or command line interface, refer to the *AT-S63 Management Software Menus Interface User's Guide* or the *AT-S63 Management Software Command Line Interface User's Guide*. The guides are available from the Allied Telesyn web site.

For background information and guidelines on the features of the AT-9400 Series switches and the AT-S63 management software, refer to the appropriate chapter in the *AT-S63 Management Software Menus Interface User's Guide*. This guide also contains an overview of the different methods to managing a switch.

This preface contains the following sections:

- ❒ "How This Guide is Organized" on page 18
- ❒ "Document Conventions" on page 19
- ❒ "Where to Find Web-based Guides" on page 20
- ❒ "Contacting Allied Telesyn" on page 21
- ❒ "New Features in AT-S63 Version 1.2.0" on page 22

Caution

The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a "retail encryption item" in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesyn sales representative for current information on this product's export status.

How This Guide is Organized

This guide is organized into the following sections

- Section I: Basic Operations

  The chapters in this section explain how to start a management session and perform basic tasks including how to configure port parameters, set up SNMPv1 and SNMPv2c, access enhanced stacking, and create port trunks and a port mirror.

- Section II: Advanced Operations

  This section includes information about the file system, uploading and downloading files, using the event log, and working with classifiers, Quality of Service, IGMP, and Denial or Service prevention.

- Section III: SNMPv3

  The chapter in this section contains the procedures for configuring SNMPv3.

- Section IV: Spanning Tree Protocols

  The chapters in this section contain the procedures for configuring the Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree Protocols.

- Section V: Virtual LANs

  The chapters in this section cover port-based and tagged VLANs, GVRP, multiple VLAN modes, and protected ports VLANs.

- Section VI: Port Security

  This section includes chapters on MAC address-based port security and 802.1x port-based network access control.

- Section VII: Management Security

  This section contains chapters about encryption keys, PKI, Secure Shell, TACACS+ and RADIUS, and the management access control list.

Note
The web browser interface supports a subset of the management functions of the switch. For a list of the management tasks that are not available from this interface, refer to “Web Browser Interface Restrictions” on page 35. Those management tasks that cannot be performed from the web browser interface can be performed from the menus and command line interfaces.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in portable document format (PDF) on our web site at **www.alliedtelesyn.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base: **http://kb.alliedtelesyn.com**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesyn without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn Technical Support through our web site: **www.alliedtelesyn.com**.

Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information through our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- Allied Telesyn web site: **www.alliedtelesyn.com**
- Allied Telesyn FTP server: **ftp://ftp.alliedtelesyn.com**

If you prefer to download new software from the Allied Telesyn FTP server from your workstation's command prompt, you will need FTP client software and you must log in to the server. Enter "anonymous" for the user name and your email address for the password.

New Features in AT-S63 Version 1.2.0

Table 1 lists the new features in version 1.2.0 of the AT-S63 management software and includes pages references to the relevant procedures. (Only one of the new features in version 1.2.0, the Supplicant Mode parameter for 802.1x authenticator ports, is supported in the web browser interface.)

Table 1. New Features in AT-S63 Version 1.2.0

Change	Chapter and Procedure
MAC Address Table	
Added new parameters to the CLI commands for deleting and displaying specific types of MAC addresses in the MAC address table. The new parameters are: ❒ STATIC, STATICUNICAST, and, STATICMULTICAST for displaying and deleting static unicast and multicast MAC addresses. ❒ DYNAMIC, DYNAMICUNICAST, and, DYNAMICMULTICAST for displaying and deleting dynamic unicast and multicast MAC addresses.	The web interface supports displaying MAC addresses, as explained in Chapter 6, “MAC Address Table” on page 93, but not the new parameters. The new parameters are only supported in the CLI interface.
Quality of Service - Flow Groups and Traffic Classes	
Added the following new parameters to QoS flow groups and traffic classes: ❒ ToS parameter for replacing the Type of Service field of IPv4 packets. ❒ Move ToS to Priority parameter for replacing the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. ❒ Move Priority to ToS parameter for replacing the value in the ToS priority field with the 802.1p priority field on IPv4 packets.	The web browser interface supports the management of flow groups and traffic classes, as explained in Chapter 15, “Quality of Service” on page 191, but not the new parameters. The new parameters are supported in the menus and command line interfaces.

Table 1. New Features in AT-S63 Version 1.2.0

Change	Chapter and Procedure
❒ **Quality of Service - Policies**	
Added the following new parameters to QoS policies: ❒ ToS, Move ToS to Priority, and Move Priority to ToS, as defined above. ❒ Send to Mirror Port parameter for copying traffic to a destination mirror port. (This parameter applies only to QoS policies.)	The web browser interface supports the management of policies, as explained in Chapter 15, "Quality of Service" on page 191, but not the new parameters. The new parameters are supported in the menus and command line interfaces.
MLD Snooping	
New feature.	This feature is not supported in the web browser interface, but is supported in the menus interface and command line interface.
MAC address-based VLANs	
New feature.	This feature is not supported in the web browser interface, but is supported in the menus interface and command line interface.
802.1x port-based network access control	
Added the following new parameter to an authenticator port: ❒ Supplicant Mode for supporting multiple supplicant accounts on an authenticator port.	Chapter 25, "802.1x Port-based Network Access Control" on page 397 Modified procedure: "Configuring Authenticator Port Parameters" on page 401

Section I

Basic Operations

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- Chapter 1, “Starting a Web Browser Management Session” on page 27
- Chapter 2, “Basic Switch Parameters” on page 37
- Chapter 3, “Enhanced Stacking” on page 55
- Chapter 4, “SNMPv1 and SNMPv2c” on page 63
- Chapter 5, “Port Parameters” on page 77
- Chapter 6, “MAC Address Table” on page 93
- Chapter 7, “Static Port Trunks” on page 103
- Chapter 8, “Port Mirroring” on page 113

Chapter 1

Starting a Web Browser Management Session

This chapter contains the procedure for starting, using, and quitting a web browser management session on an AT-9400 Series switch. Sections in the chapter include:

- ❒ "Establishing a Remote Connection to Use the Web Browser Interface" on page 28
- ❒ "Web Browser Tools" on page 31
- ❒ "Saving Your Parameter Changes" on page 32
- ❒ "Quitting a Web Browser Management Session" on page 33
- ❒ "Ports 23R and 24R on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series Switches" on page 34
- ❒ "Web Browser Interface Restrictions" on page 35

Establishing a Remote Connection to Use the Web Browser Interface

To establish a web browser management session with an AT-9400 Series switch, the switch must be part of an enhanced stack or it must have an IP address and subnet mask. If the switch is part of an enhanced stack, such as a slave switch, start the web browser management session on the stack's master switch. After you have started the session, you can access and manage all of the switches in the stack from the master switch.

If the switch is not part of an enhanced stack and does not have an IP address and you want to manage it with the web browser interface, you must give it an IP address. This is initially assigned through a local connection to the switch using the Terminal Port on the switch and either the menus or the command line interface (CLI). After an IP address and subnet mask are assigned, you can remotely connect to the switch and start a web browser management session.

Note
For background information on enhanced stacking, refer to Chapter 4, "Enhanced Stacking," in the *AT-S63 Management Software Menus Interface User's Guide*.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

Note
If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser to not use proxies.

2. In the URL field of the browser, enter the IP address of the switch you want to manage or of the master switch of the enhanced stack.

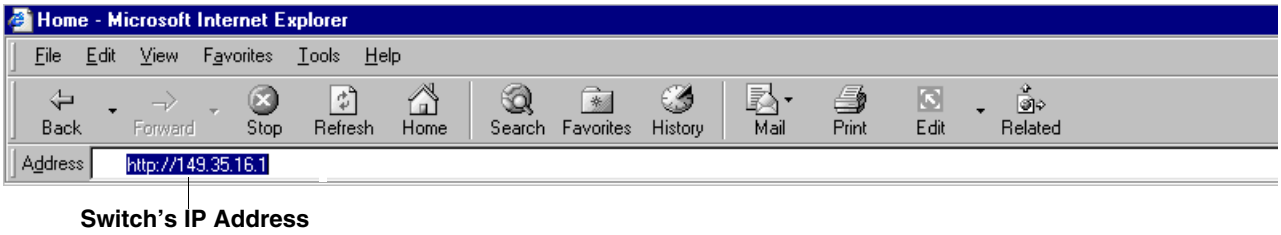
Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Related
Address http://149.35.16.1
Switch's IP Address

Figure 1. Entering a Switch's IP Address in the URL Field

The AT-S63 management software displays the login page, shown in Figure 2.

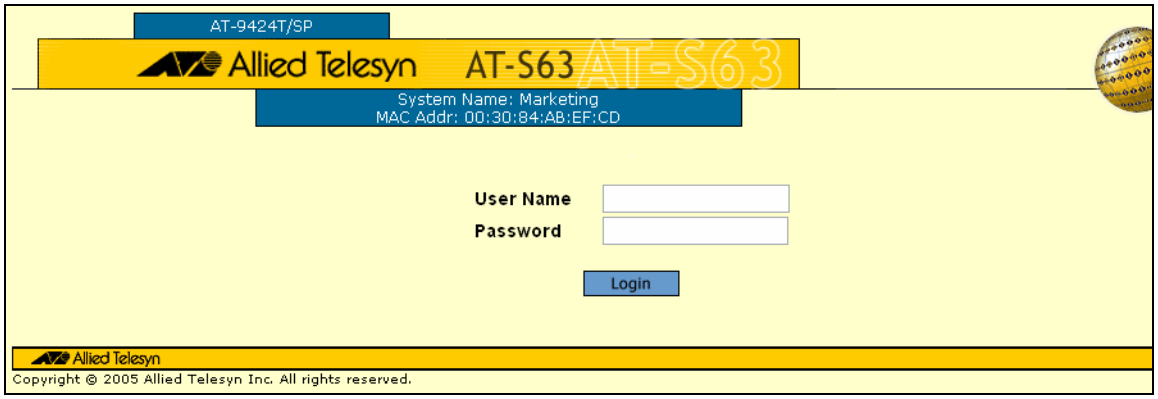

Figure 2. AT-S63 Login Page

3. Enter a user name and password. For manager access, enter "manager" as the user name. The default password is "friend." For operator access, enter "operator" as the user name. The default password is "operator." Login names and passwords are case-sensitive. (For information about the two access levels, refer to "Management Access" in Chapter 1, "Overview," of the *AT-S63 Management Software Menus Interface User's Guide*.)

   You cannot change the default user names. To change a password, refer to "Configuring the Manager and Operator Passwords" on page 44.

   The home page is shown in Figure 3.

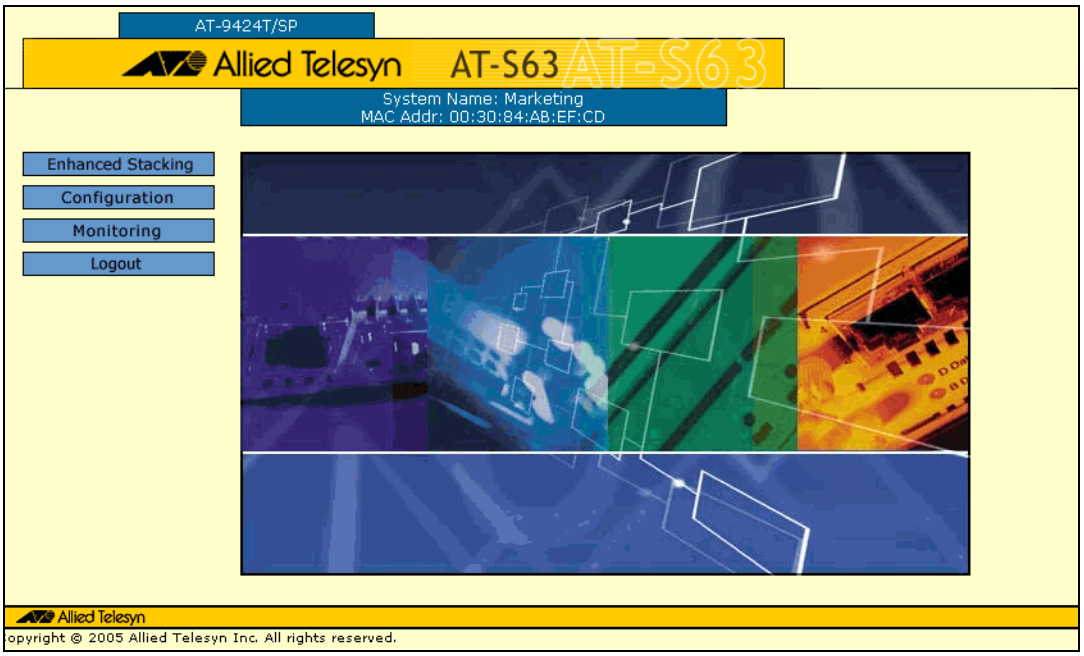

Figure 3. Home page

The main menu is on the left side of the home page. It consists of the following selections:

- ❒ Enhanced Stacking
- ❒ Configuration
- ❒ Monitoring
- ❒ Logout

Note
The Enhanced Stacking selection is included in the menu only if the switch you accessed is a master switch.

A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

You should always log out from a web browser management session when you are finished managing a switch. (For instructions, see “Quitting a Web Browser Management Session” on page 33.) Logging out prevents unauthorized individuals from making changes to a switch’s configuration if you leave your management station unattended. Also, as long as you are logged in, no one else can access the switch through another local or remote connection.

If you close your web browser without logging out, the switch considers the management session as still in progress and will not permit the start of another management session until the expiration of the console timer. The timer is used to end inactive local and remote management sessions. The default setting for the timer is ten minutes. The console timer can be set from the menus or the command line interface, but not from the web browser interface.

Web Browser Tools

You can use the web browser tools to move around the management pages. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature to save the link to the switch.

Saving Your Parameter Changes

When you make a change to a switch parameter, the change is, in most cases, immediately activated as soon as you click the Apply button on the web page. However, a change to a switch parameter is initially saved only to temporary memory. It is lost the next time you reset or power cycle the unit. To permanently save a change, you must click the **Save Config** option on the Configuration menu, shown in Figure 4. Selecting the option updates the switch's active configuration file. A change saved to the active configuration file is retained even when the unit is powered off or reset. This menu option is displayed only after you have made configuration changes. After you click **Save Config**, your changes are added to the active configuration file and the option is removed from the menu.

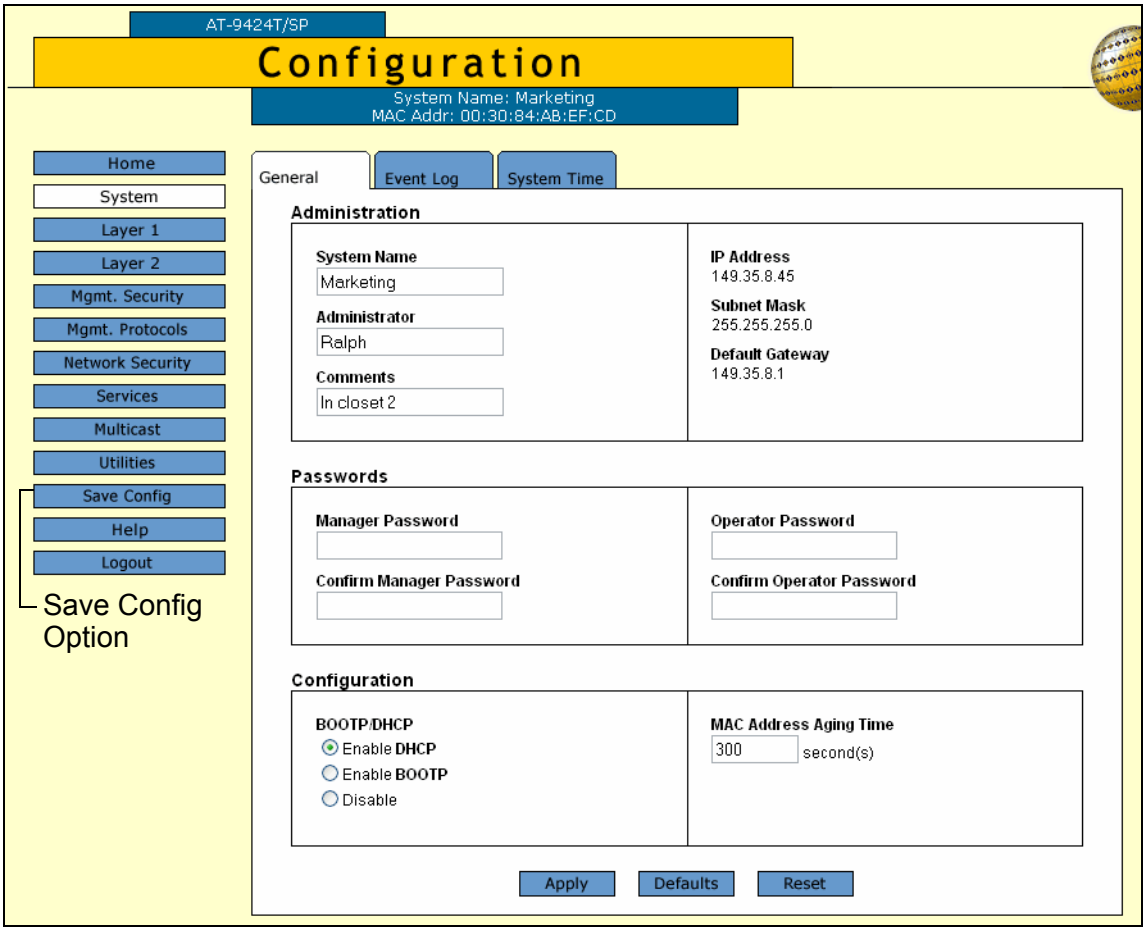

Figure 4. Save Config Option in the Configuration Menu

Quitting a Web Browser Management Session

To exit a web browser management session, select the **Logout** option from the main menu.

Ports 23R and 24R on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series Switches

This section applies to the twisted pair ports 23R and 24R and the SFP and GBIC slots on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series switches. Note the following when configuring these ports:

- Twisted pair ports 23R and 24R change to the redundant status mode when an SFP or GBIC module is installed and establishes a link with its end node. An SFP or GBIC port is only active while it has a valid link. At all other times the corresponding twisted pair port 23R or 24R is the active port.
- A twisted pair port and its corresponding SFP or GBIC module share the same configuration settings, including port settings, VLAN assignments, access control lists, and spanning tree. When an SFP or GBIC module becomes active, it operates with the same settings as its corresponding twisted pair port.
- An exception is port speed: If you disable Auto-Negotiation on twisted pair port 23R or 24R and set the speed and duplex mode manually, the speed reverts to Auto-Negotiation when you install an SFP or GBIC module and the module establishes a link with an end node.

Web Browser Interface Restrictions

The following management tasks of the AT-S63 management software are not support in the web browser interface. These functions must be performed from the menus interface or the command line interface.

- Configuring the console timer
- Forcing a port to renegotiate its settings with a remote node
- Configuring LACP port trunks
- Viewing the networking stack
- Configuring MAC address-based VLANs
- Copying, renaming, and deleting files from the file system or from a compact flash memory card
- Changing directories on a compact flash memory card
- Uploading or downloading files to a compact flash memory card
- Creating a new switch configuration file
- Modifying the event log full action
- Configuring MLD snooping
- Configuring RRP snooping
- Creating, deleting, importing, and exporting encryption keys
- Creating SSL self-signed certificates
- Generating an SSL certificate enrollment request
- Copying SSL certificates into the certificate database or modifying certificates
- Formatting flash memory
- Transferring the AT-S63 image file or a configuration file from a master switch to a slave switch (i.e., switch to switch upload)
- Configuring the Type of Service, Move ToS to Priority, Move Priority to ToS, and Send to Mirror Port parameters in QoS flow groups, traffic classes, and policies
- Adjusting the baud rate on the serial terminal port
- Enabling and disabling the Telnet server
- Configuring the Telnet NULL character parameter
- Configuring the console startup mode
- Configuring the web browser server

Chapter 2

Basic Switch Parameters

This chapter contains the following sections:

- “Configuring an IP Address and Switch Name” on page 38
- “Activating the BOOTP or DHCP Client Software” on page 41
- “Displaying System Information” on page 42
- “Configuring the Manager and Operator Passwords” on page 44
- “Rebooting a Switch” on page 46
- “Setting the System Date and Time” on page 47
- “Pinging a Remote System” on page 50
- “Returning the AT-S63 Management Software to the Factory Default Values” on page 52

Configuring an IP Address and Switch Name

Note
For guidelines about when to assign an IP address, subnet address, and gateway address to an AT-9400 Series switch, refer to "When Does a Switch Need an IP Address?" in Chapter 3, "Basic Switch Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

To set basic switch parameters for an AT-9400 Series switch, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5.

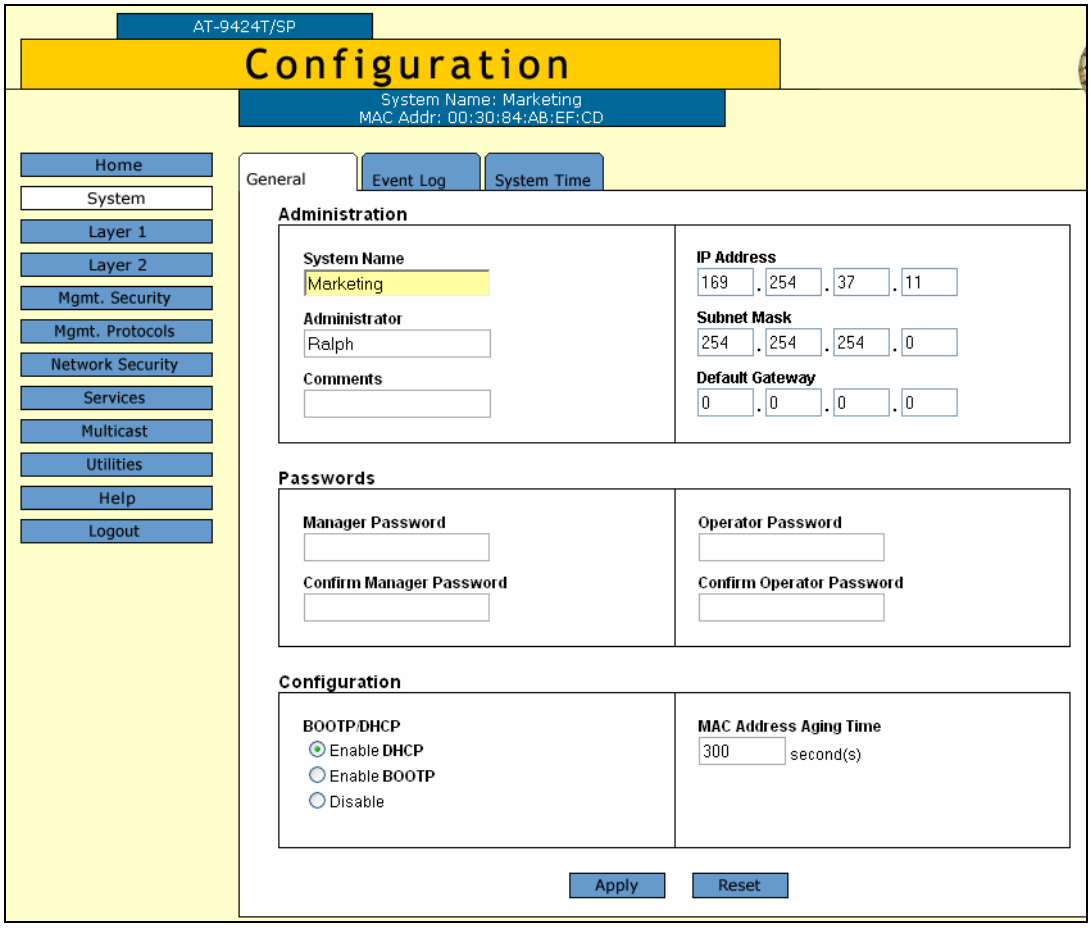

Figure 5. General Tab (Configuration)

Note
This procedure describes the parameters in the Administration section of the tab. The Passwords section is described in "Configuring the Manager and Operator Passwords" on page 44. The BOOTP/DHCP parameters are described in "Activating the BOOTP or DHCP Client Software" on page 41. The MAC Address Aging Time parameter is described in "Changing the Aging Time" on page 101.

Note
The Reset button resets the switch. For instructions, refer to "Rebooting a Switch" on page 46.

2. Configure the following parameters as necessary:

System Name
This parameter specifies a name for the switch (for example, Sales Ethernet switch). The name is displayed at the top of the AT-S63 management pages and tabs. The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.

Note
Allied Telesyn recommends assigning each switch a name. Names make it easier for you to identify the various switches when you manage them, and they can help you avoid performing a configuration procedure on the wrong switch.

Administrator
This parameter specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 20 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

Comments
This parameter specifies the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.

Note
The following three parameters are used to manually assign the switch an IP address, subnet mask, and default gateway. An alternative method to configuring these parameters is with a DHCP or BOOTP server, which can assign values to these parameters automatically. See “Activating the BOOTP or DHCP Client Software” on page 41, and information in Chapter 3, “Basic Switch Parameters” in the *AT-S63 Management Software Menus Interface User’s Guide*.

IP Address
This parameter specifies the IP address of the switch. You must specify an IP address if you want the switch to function as the Master switch of an enhanced stack. The IP address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Subnet Mask
This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch. The subnet mask must be entered in the format: xxx.xxx.xxx.xxx. The default value is 255.255.0.0.

Default Gateway
This parameter specifies the default router’s IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router. The address must be entered in the format: xxx:xxx:xxx:xxx. The default value is 0.0.0.0.

3. Click **Apply** to activate your changes on the switch.

Note
A change to any of the above parameters is immediately activated on the switch.

A change to the IP address of the switch results in the loss of a remote management session. You can restart the management session using the switch’s new IP address.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Activating the BOOTP or DHCP Client Software

For background information on BOOTP and DHCP, refer to Chapter 3, "Basic Switch Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

To activate or deactivate the BOOTP or DHCP client software on the switch from a web browser management session, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. In the Configuration section, for the **BOOTP/DHCP** parameter, click one of the following:

   Enable DHCP
   Enables DHCP.

   Enable BOOTP
   Enables BOOTP.

   Disable
   Disables both DHCP and BOOTP. This is the correct setting if you want to enter a static IP address for the switch or do not want to assign the switch an IP address. The default is disabled.

3. Click **Apply** to activate your change on the switch.

   Note
   If you enabled BOOTP or DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response. If you manually assigned an IP address to the switch, that address is deleted and replaced by the IP address received from the BOOTP or DHCP server.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying System Information

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6.

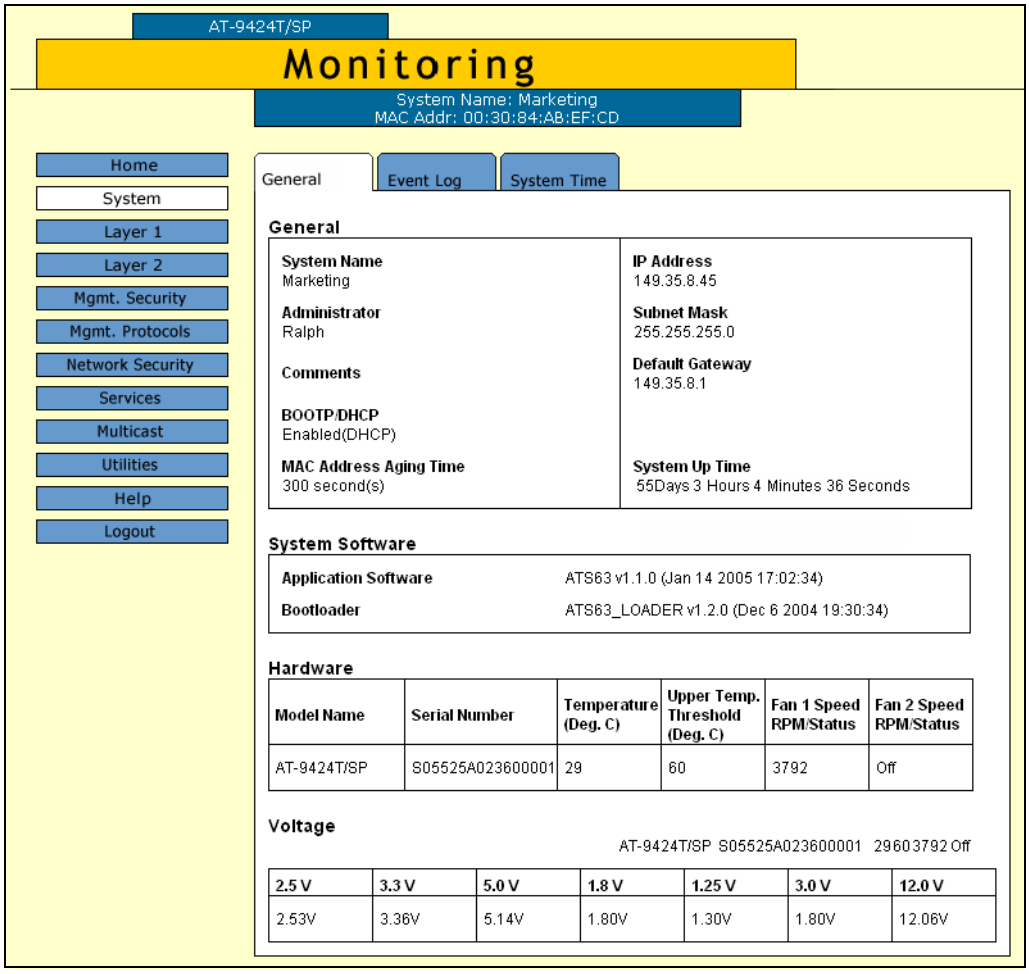

Figure 6. General Tab (Monitoring)

The General section displays the following information:

System Name
The name of the switch.

Administrator
The name of the network administrator responsible for managing the switch.

Comments
The location of the switch, (for example, 4th Floor - rm 402B).

BOOTP/DHCP
The status of the BOOTP and DHCP client software. If enabled, the switch is obtaining its IP information from a BOOTP or DHCP server on the network.

MAC Address Aging Time
The time interval an inactive dynamic MAC address can remain in the MAC address table before it is deleted.

IP Address
The switch's IP address.

Subnet Mask
The switch's subnet mask.

Default Gateway
The IP address of a router for remote management.

System Up Time
The length of time since the switch was last reset or power cycled.

The System Software section displays the following information:

Application Software
The version number and build date of the AT-S63 management software.

Bootloader
The version number and build date of the AT-S63 bootloader.

The Hardware section displays the following information:

Model Name
The model name.

Serial Number
The switch serial number.

Temperature (Deg.C)
The current system temperature.

Upper Temp. Threshold (Deg C)
The upper threshold for the switch temperature.

Fan 1 Speed RPM/Status
Fan 2 Speed RPM/Status
The speed or operating status of the system fan(s).

The Voltage section provides the current voltage of the six power supplies in the switch, identified as 2.5 V, 3.3 V, 5 V, 1.8 V, 1.25 V, and 12 V.

Configuring the Manager and Operator Passwords

There are two levels of management access on an AT-9400 Series switch: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate username and password when you start an AT-S63 management session. The default password for manager access is "friend." The default password for operator access is "operator." Passwords are case sensitive.

To change the manager or operator password, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. In the Passwords section, enter the new values. The parameters are described below.

   Manager Password
   Confirm Manager Password
   You use these parameters to change the manager's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "friend." The password is case sensitive.

Caution
Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Operator Password
Confirm Operator Password
Use these parameters to change the operator's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password for operator is "operator." The password is case sensitive.

Caution
Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Note
A change to a password is immediately activated on the switch. You are prompted for the new password the next time you log in.

3. Click **Apply** to activate your change on the switch.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Rebooting a Switch

Note
Any parameters changes that have not been saved are discarded when a system is reset. To save parameter changes, refer to “Saving Your Parameter Changes” on page 32.

To reboot a switch, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Click **Reset** at the bottom of the tab.

   A confirmation prompt is displayed.

3. Click **OK** to reset the switch or **Cancel** to cancel the procedure:

   Note
   The switch does not forward packets while it initializes the AT-S63 management software and loads its active configuration file. This process takes between 20 seconds to 2 minutes to complete, depending on the number and types of commands in the configuration file.

   Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Setting the System Date and Time

This procedure explains how to set the switch's date and time. Setting the date and time is important if you plan to view the events in the switch's event log or send the events to a syslog server. The correct date and time are also important if the management software will be sending traps to your management workstation or if you plan to create a self-signed SSL certificate. Events, traps, and self-signed certificates should contain the date and time of when they occurred or, in the case of certificates, when they were created.

There are two ways that you can set the switch's date and time. One method is to set it manually. The AT-9400 Series switch has an onboard battery that maintains the date and time even when the unit is powered off or reset.

The second method uses the Simple Network Time Protocol (SNTP). The AT-S63 management software comes with the client version of this protocol. You can configure the AT-S63 software to obtain the current date and time from an SNTP or Network Time Protocol (NTP) server located on your network or the Internet.

SNTP is a reduced version of the NTP. However, the SNTP client software in the AT-S63 management software is interoperable with NTP servers.

Note
The default system time on the switch is midnight, January 1, 1980.

To set the system time manually or to configure SNTP client, do the following:

1. From the Home Page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **System Time** tab.

The System Time tab is shown in Figure 7.

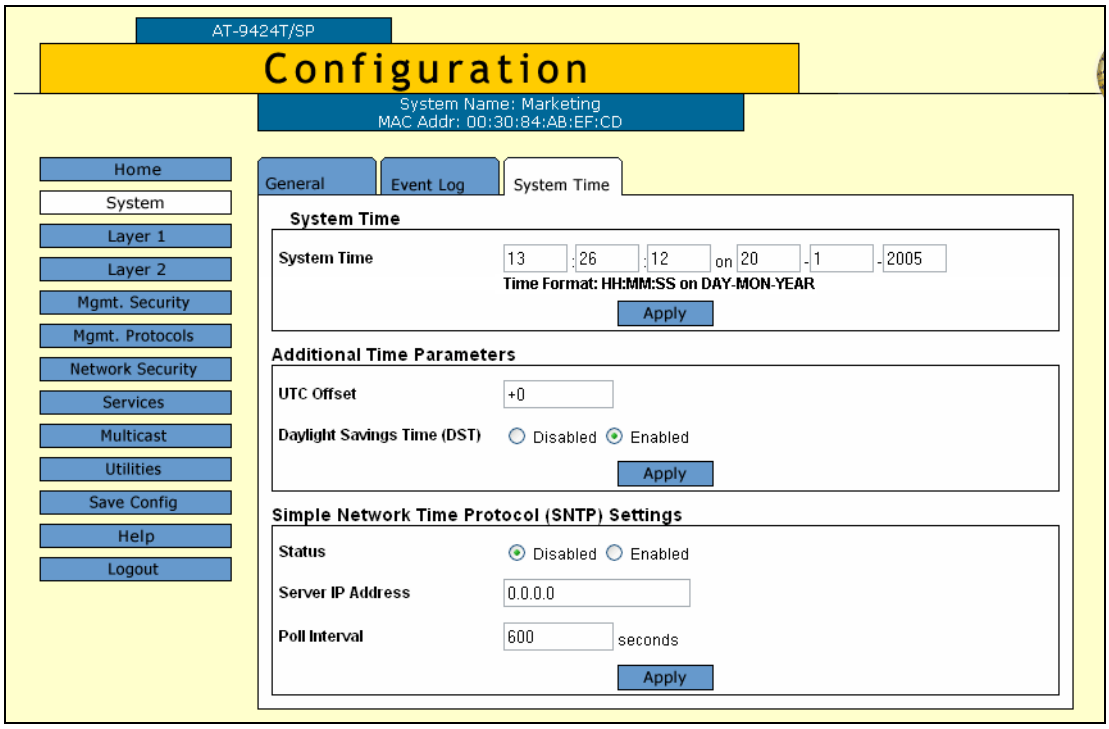

Figure 7. System Time Tab

3. To set the system time manually, do the following:

   a. In the System Time section of the tab, enter the time and date in the following format.

      hh:mm:ss dd-mm-yyyy

   b. Click **Apply**.

4. To configure the switch to obtain its date and time from an SNTP or NTP server on your network or the Internet, configure the following options:

   UTC Offset
   Specifies the difference between the UTC and local time. The default is 0 hours. The range is -12 to +12 hours.

   Note
   If the switch is using DHCP, it automatically attempts to determine this value. In this case, you do not need to configure a value for the UTC Offset parameter.

Daylight Savings Time (DST)
Enables or disables the system's adjustment for daylight savings time. The default is enabled.

> **Note**
> The switch does not set DST automatically. If the switch is in a locale that uses DST, you must remember to enable this in April when DST begins and disable it in October when DST ends. If the switch is in a locale that does not use DST, this option should be set to disabled all the time.

Status
Enables or disables the SNTP client on the switch. The default is disabled.

Server IP Address
Specifies the IP address of an SNTP server.

> **Note**
> If the switch is obtaining its IP address and subnet mask from a DHCP sever, you can configure the DHCP server to provide the switch with an IP address of an NTP or SNTP server. If you configured the DHCP server to provide this address, then you do not need to enter it here.

Poll Interval
Specifies the number of seconds the switch waits between polling the SNTP or NTP server. The default is 600 seconds. The range is from 60 to 1200 seconds.

5. When you finish configuring the parameters, click the **Apply** buttons.

> **Note**
> If you enabled the SNTP client, the switch immediately polls the SNTP or NTP server for the current date and time. (The switch automatically polls the server whenever a change is made to any of the parameters in this menu, so long as SNTP is enabled.)

6. To permanently save your changes to the SNTP client, click **Save Config**.

Pinging a Remote System

You can instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Utilities** option.

   The Utilities tab is displayed with the File System tab selected by default, as shown in Figure 8.

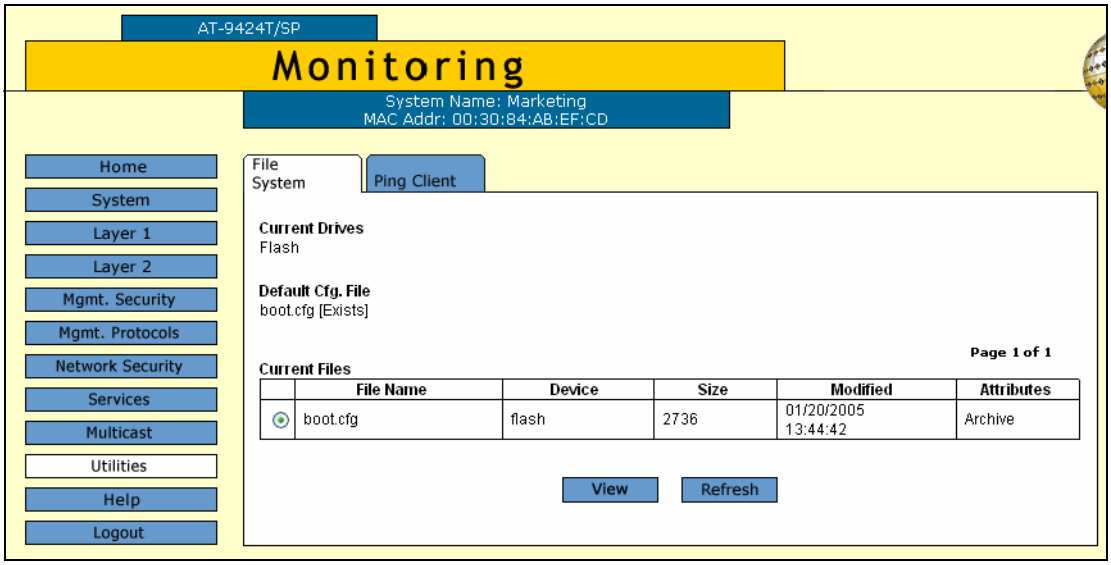

Figure 8. File System Tab (Monitoring)

3. Select the **Ping Client** tab.

The Ping Client tab is shown in Figure 9.

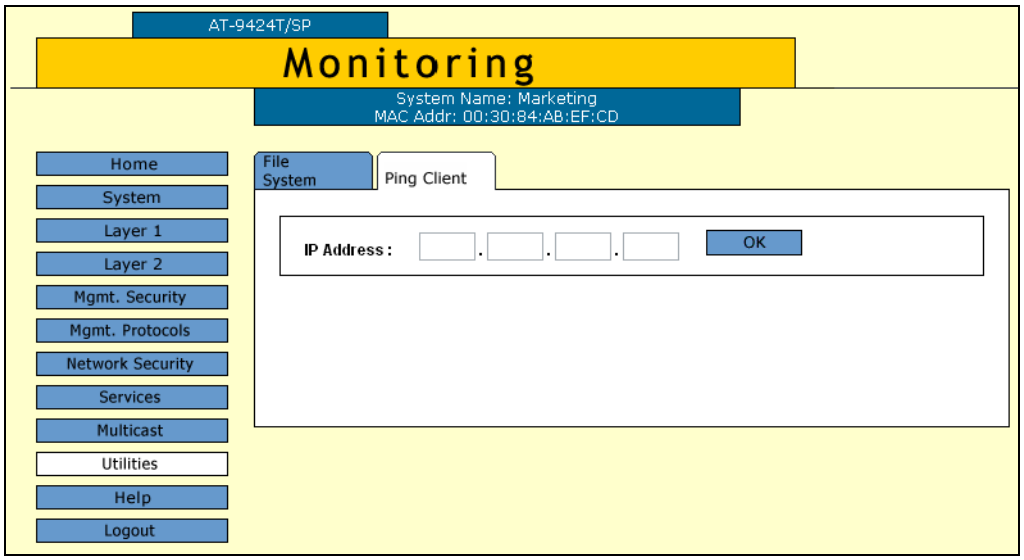

Figure 9. Ping Client Tab (Monitoring)

4. Enter the IP address of the end node you want the switch to ping.
5. Click **OK**.

   The results of the ping are displayed in a popup window.
6. To stop the ping, click **OK**.

Returning the AT-S63 Management Software to the Factory Default Values

The procedure in this section returns all AT-S63 management software parameters to their default values. Please note the following before you perform this procedure:

- Returning all parameter settings to their default values also deletes any port-based or tagged VLANs you created on the switch.
- This procedure does not delete files from the AT-S63 file system. To delete files, refer to Chapter 11, “File System,” in the *AT-S63 Management Software Menus Interface User’s Guide*.
- This procedure does not delete any encryption keys stored in the key database. To delete encryption keys, refer to “Deleting a Key,” in Chapter 33, “Encryption Keys,” in the *AT-S63 Management Software Menus Interface User’s Guide*.
- If you manually assigned the unit an IP address and subnet mask, they are deleted.
- DHCP and BOOTP are disabled.
- Returning a switch to its default values does not alter the contents of the active boot configuration file. To reset the file back to the default settings, you must select Save Config from the menu after the switch reboots and you reestablish your management session. Otherwise, the switch reverts back to the previous configuration the next time you reset or power cycle the unit.
- The speed of the Terminal Port on the switch is not changed.

Please note the following when performing this procedure on a master switch of an enhanced stack:

- You will not be able to reestablish your web browser management session on the unit at the completion of this procedure because the unit will not have an IP address and its stacking status will be slave, the default setting. Unless there is another master switch in the same subnet, you must use a local management session if you want to continue managing the switch at the completion of this procedure.
- The management VLAN setting is returned to Default_VLAN.

Caution

This procedure involves a switch reset. Some network traffic may be lost while the unit initializes its management software and loads the default configuration settings, a process that takes approximately 20 seconds to complete.

Note
The AT-S63 management software default values are listed in Appendix A, "AT-S63 Default Settings" in the *AT-S63 Management Software Menus Interface User's Guide*.

To return the AT-S63 management software to the default settings, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab selected by default, as shown in Figure 10.

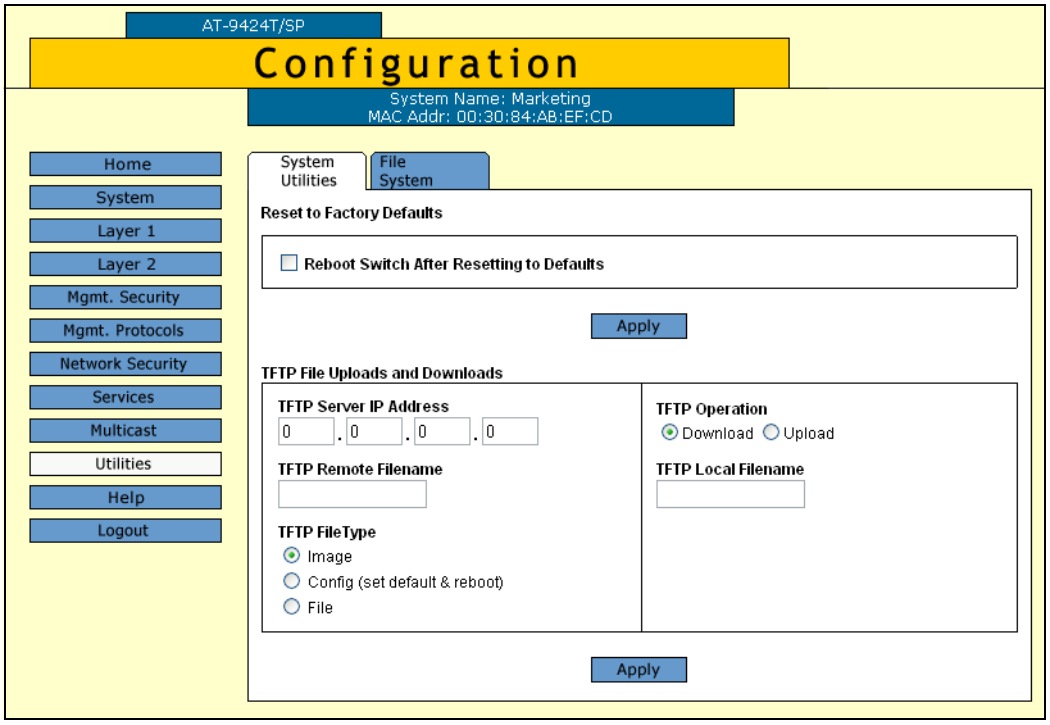

Figure 10. System Utilities Tab (Configuration)

3. Click the **Reboot Switch After Resetting to Defaults** checkbox.

4. Click **Apply**.

   The web browser displays the following prompt:

   ```
   This page may no longer be available while the switch
   reboots. Do you want to continue?
   ```

5. Click **OK** to continue, or **Cancel** to cancel the procedure.

   If you select OK, the switch resets and returns all values to the default settings. After the reset is complete, you must reestablish your management session if you want to continue managing the unit.

   As mentioned at the start of this procedure, returning a switch to is default settings does not alter the contents of the active boot configuration file. To return the file to the default settings, you must save the current switch settings after you reestablish your management session. Otherwise, the switch returns to its previous parameter settings the next time you reset or power cycle the unit.

Chapter 3

Enhanced Stacking

This chapter contains the following procedures for setting up enhanced stacking:

- ❒ “Setting a Switch’s Enhanced Stacking Status” on page 56
- ❒ “Selecting a Switch in an Enhanced Stack” on page 58
- ❒ “Returning to the Master Switch” on page 61
- ❒ “Displaying the Enhanced Stacking Status” on page 62

Note
For background information on enhanced stacking, refer to Chapter 4, “Enhanced Stacking,” in the *AT-S63 Management Software Menus Interface User’s Guide.*

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- Master - A master switch of a stack can be used to manage other enhanced stacking switches in a subnet. After you have established a local or remote management session with the master switch, you can access and manage the other enhanced stacking switches in the subnet.

  In order to manage the switches of an enhanced stack using the web browser interface, you must assign the master switch a unique IP address. You can manually assign the address or activate the BOOTP or DHCP client software on the switch so that it automatically obtains an IP address from a BOOTP or DHCP server on your network. Refer to "Configuring an IP Address and Switch Name" on page 38 and "Activating the BOOTP or DHCP Client Software" on page 41 for further information.

- Slave - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.
- Unavailable - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note
The default setting for a switch is slave.

Note
The only switch whose stacking status you can change through a web browser management session is the switch where you started the management session, typically a master switch. You cannot change the stacking status of a switch accessed through enhanced stacking. If the switch does not have an IP address and subnet mask, you must use a local management session to change its stacking status.

To configure a switch's enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **Enhanced Stacking** tab.

   The Enhanced Stacking tab is shown in Figure 11.

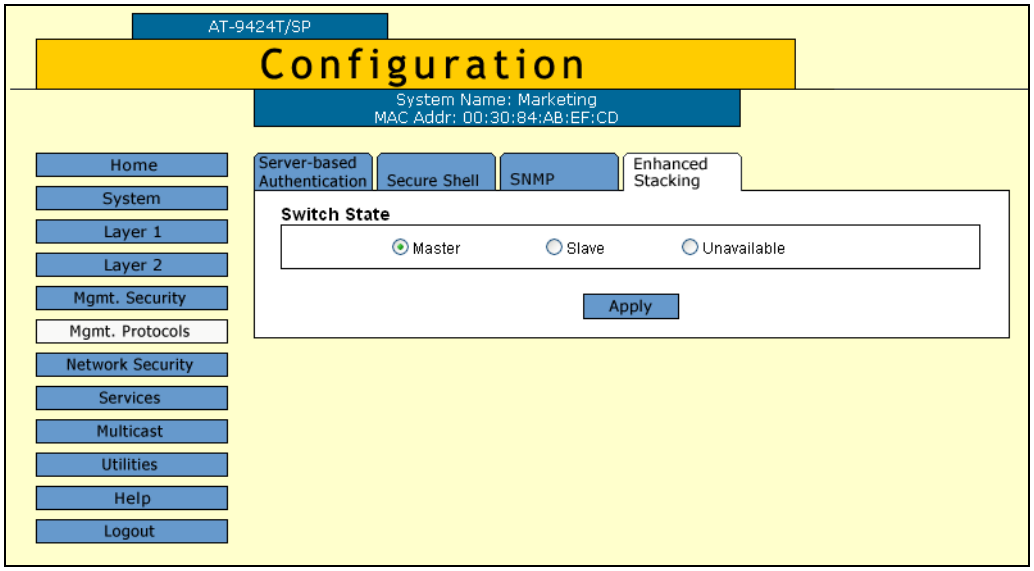

Figure 11. Enhanced Stacking Tab (Configuration)

4. Click the desired enhanced stacking status for the switch. The default is Slave.

5. Click **Apply**.

   The new enhanced stacking status is immediately activated on the switch.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Selecting a Switch in an Enhanced Stack

Before you perform any procedure on a switch in an enhanced stack, check to be sure that you are performing it on the correct switch. If you assigned system names to your switches, identifying your switches is easy. The AT-S63 management software displays the name of the switch being managed at the top of every management menu.

When you start a web browser management session on the master switch of the enhanced stack, you are by default addressing that particular switch. The management tasks that you perform affect only the master switch.

To manage a slave switch or another master switch in the same stack, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the home page, select **Enhanced Stacking**.

   Note
   If the Home page does not have an Enhanced Stacking menu option, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure:

   The master switch polls the network for the slave and master enhanced stacking switches in the subnet and displays a list of the switches in the Stacking Switches page. An example is shown in Figure 12.

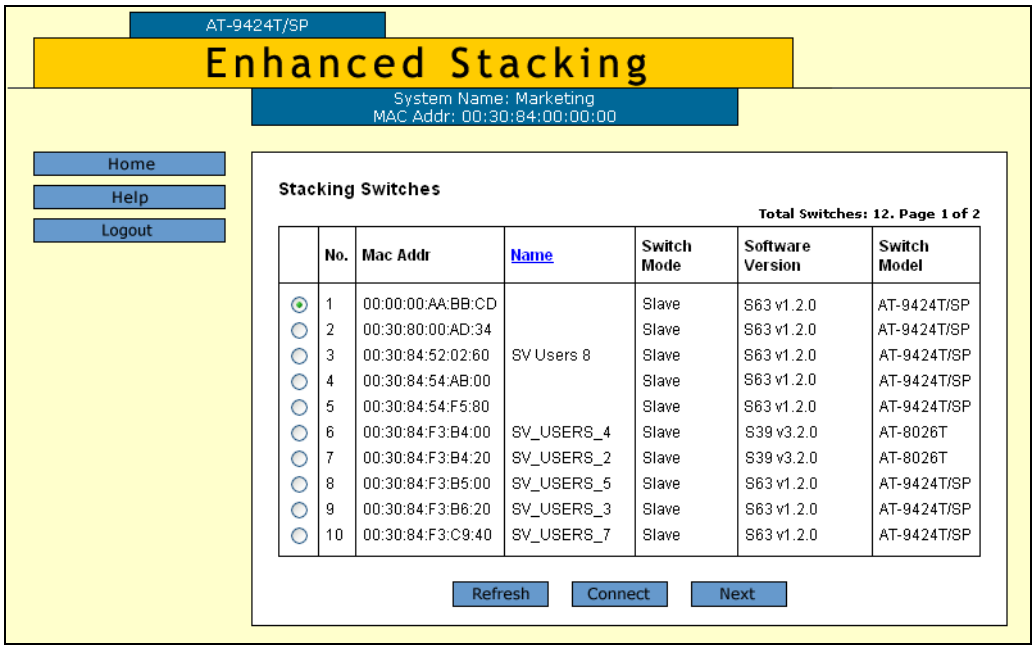
AT-9424T/SP
Enhanced Stacking
System Name: Marketing
MAC Addr: 00:30:84:00:00:00
Home
Help
Logout
Stacking Switches
Total Switches: 12. Page 1 of 2
No. Mac Addr Name Switch Mode Software Version Switch Model
1 00:00:00:AA:BB:CD Slave S63 v1.2.0 AT-9424T/SP
2 00:30:80:00:AD:34 Slave S63 v1.2.0 AT-9424T/SP
3 00:30:84:52:02:60 SV Users 8 Slave S63 v1.2.0 AT-9424T/SP
4 00:30:84:54:AB:00 Slave S63 v1.2.0 AT-9424T/SP
5 00:30:84:54:F5:80 Slave S63 v1.2.0 AT-9424T/SP
6 00:30:84:F3:B4:00 SV_USERS_4 Slave S39 v3.2.0 AT-8026T
7 00:30:84:F3:B4:20 SV_USERS_2 Slave S39 v3.2.0 AT-8026T
8 00:30:84:F3:B5:00 SV_USERS_5 Slave S63 v1.2.0 AT-9424T/SP
9 00:30:84:F3:B6:20 SV_USERS_3 Slave S63 v1.2.0 AT-9424T/SP
10 00:30:84:F3:C9:40 SV_USERS_7 Slave S63 v1.2.0 AT-9424T/SP
Refresh
Connect
Next

Figure 12. Stacking Switches Page

Note
The master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

To refresh the list, click **Refresh**. This instructs the master switch to again poll the subnet for all switches.

2. To manage another switch in an enhanced stack, click the button to the left of the appropriate switch in the list. You can select only one switch at a time.

Note
If the web server on the master switch is operating in the secure HTTPS mode, you can manage only those enhanced stacking switches that are also operating HTTPS. You cannot manage a switch whose web server is operating in the non-secure HTTP mode.

3. Click **Connect**.

4. Enter a user name and password for the switch when prompted.

   The home page of the selected switch is displayed. You can now manage the switch.

Returning to the Master Switch

When you are finished managing a slave switch and want to manage another switch in the stack, return to the Home page of the switch and select **Disconnect** from the menu. This returns you to the Enhanced Stacking page in Figure 12 on page 59. When you see that page, you are again addressing the master switch from which you started the management session.

You can select another switch in the list to manage or, if you want to manage the master switch, select **Home** to return to the master switch's home page.

Displaying the Enhanced Stacking Status

To display the enhanced stacking status of the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 179 on page 436.

3. Select the **Enhanced Stacking** tab.

   The Enhanced Stacking tab is shown Figure 13.

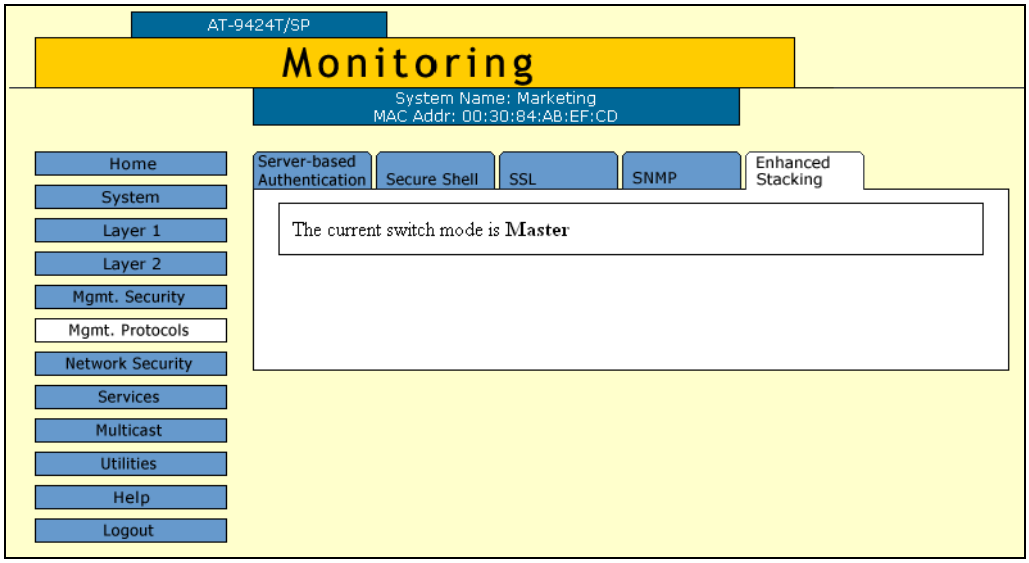

Figure 13. Enhanced Stacking Tab (Monitoring)

The information in the tab states the current enhanced stacking status of the switch as master, slave, or unavailable.

Chapter 4

SNMPv1 and SNMPv2c

This chapter explains how to activate SNMP management on the switch and how to create, modify, and delete SNMPv1 and SNMPv2c community strings. This chapter contains the following procedures:

- ❒ “Enabling or Disabling SNMP Management” on page 64
- ❒ “Creating a New SNMPv1 and SNMPv2c Community” on page 66
- ❒ “Modifying an SNMPv1 and SNMPv2c Community” on page 69
- ❒ “Deleting an SNMPv1 and SNMPv2c Community” on page 72
- ❒ “Displaying the SNMPv1 and SNMPv2c Communities” on page 73

Note
For background information about SNMPv1 and SNMPv2c, refer to Chapter 5, “SNMPv1 and SNMPv2c,” in the *AT-S63 Management Software Menus Interface User’s Guide.*

Enabling or Disabling SNMP Management

To enable or disable SNMP management on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14.

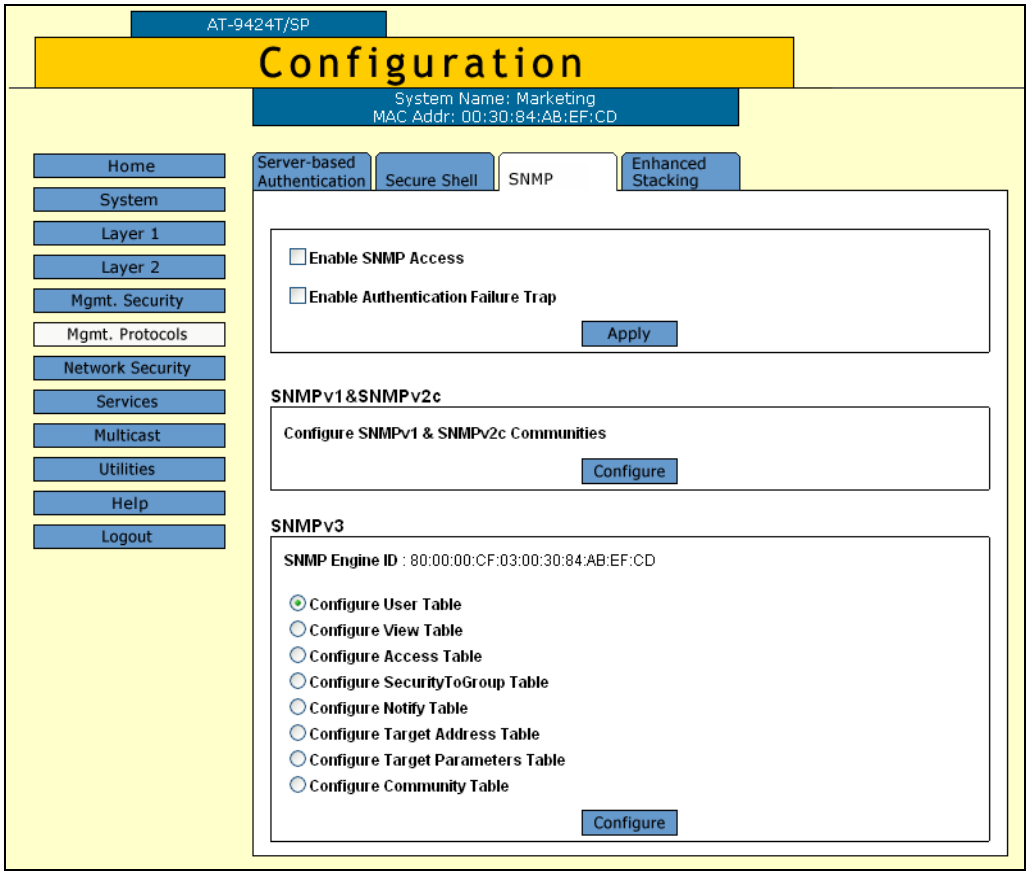

Figure 14. SNMP Tab (Configuration)

4. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.

5. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.

6. Click **Apply**.

   A change to SNMP access is immediately activated on the switch.

   The community strings that already exist on the switch are displayed in a table.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Creating a New SNMPv1 and SNMPv2c Community

To create a new SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14 on page 64.

4. In the SNMPv1 & SNMPv2c section, click **Configure**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 15.

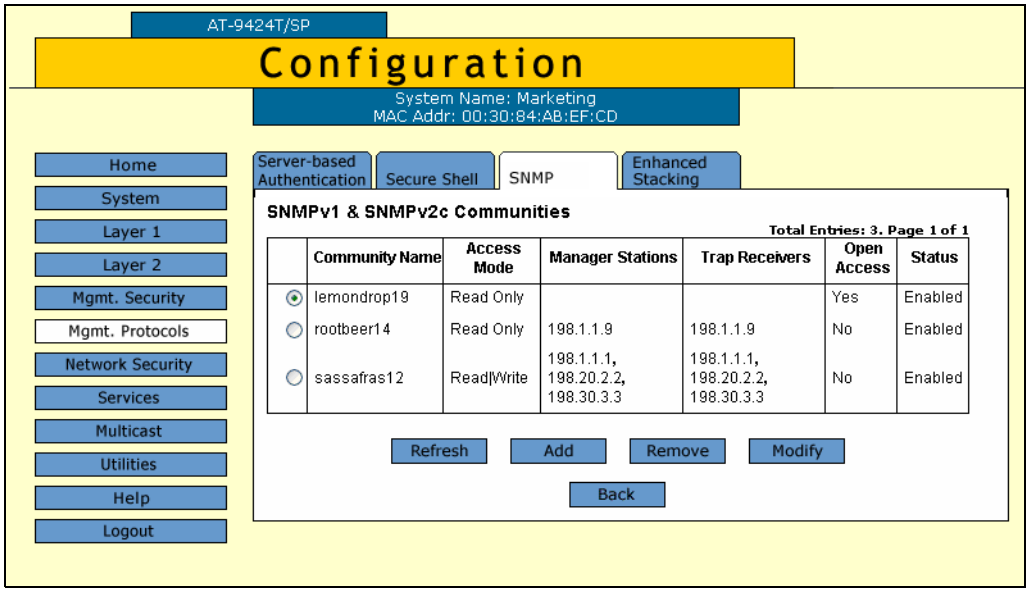

Figure 15. SNMPv1 & SNMPv2c Communities Tab

5. Click **Add**.

The Add New SNMPv1 & SNMPv2c Community page is shown in Figure 16.

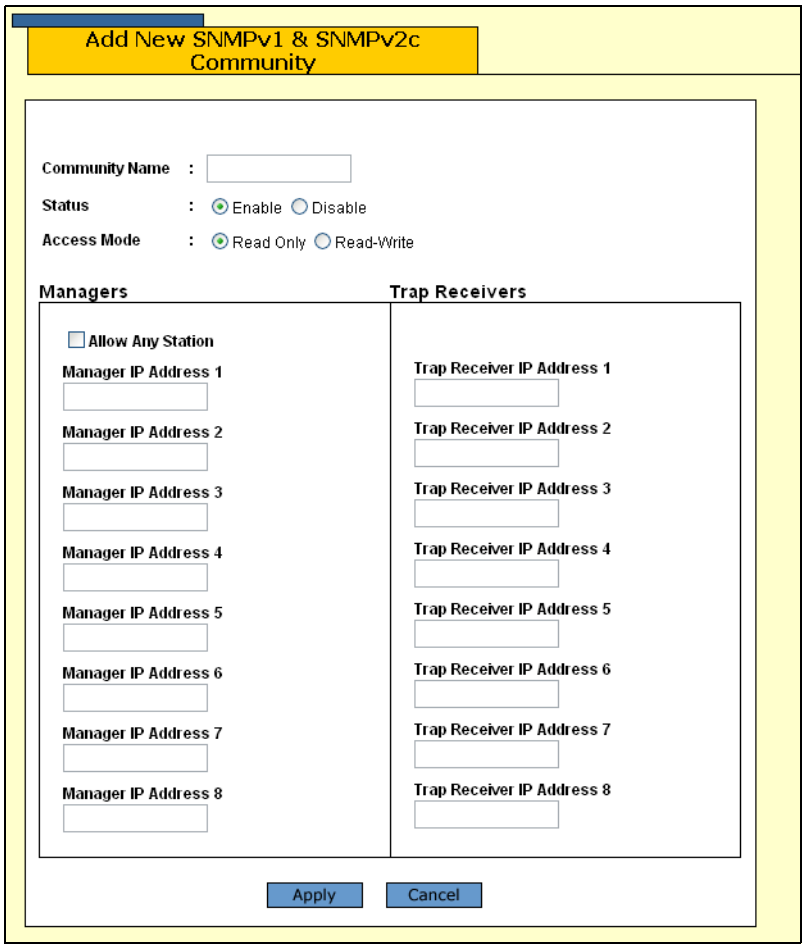
Add New SNMPv1 & SNMPv2c Community
Community Name :
Status : Enable Disable
Access Mode : Read Only Read-Write
Managers
Trap Receivers
Allow Any Station
Manager IP Address 1
Manager IP Address 2
Manager IP Address 3
Manager IP Address 4
Manager IP Address 5
Manager IP Address 6
Manager IP Address 7
Manager IP Address 8
Trap Receiver IP Address 1
Trap Receiver IP Address 2
Trap Receiver IP Address 3
Trap Receiver IP Address 4
Trap Receiver IP Address 5
Trap Receiver IP Address 6
Trap Receiver IP Address 7
Trap Receiver IP Address 8
Apply
Cancel

Figure 16. Add New SNMPv1 & SNMPv2c Community Page

6. Configure the following parameters:

Community Name
Enter an SNMP community name that consists of up to 15 alphanumeric characters.

Status
Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode
Click Read Only to allow read access to the SNMP community. To allow read-write access to the SNMP community, click Read-Write.

Allow Any Station
Click this option to allow any SNMP manager to access the switch. When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address 1 through **Manager IP Address 8**
Enter an IP Address of a switch that is permitted SNMP manager access to the current switch. You can enter up to eight Manager IP Addresses.

Trap Receiver IP Address 1 through **Trap Receiver IP Address 8**
Use the above selections to specify the IP addresses of up to eight trap receivers on your network that can receive traps from the switch.

7. Click **Apply**.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an SNMPv1 and SNMPv2c Community

To modify an SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14 on page 64.

4. In the SNMPv1 & SNMPv2c section, click **Configure**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 15 on page 66.

5. Click the button next to the community name and click **Modify**.

   The Modify SNMPv1 & SNMPv2c Community page is shown in Figure 17.

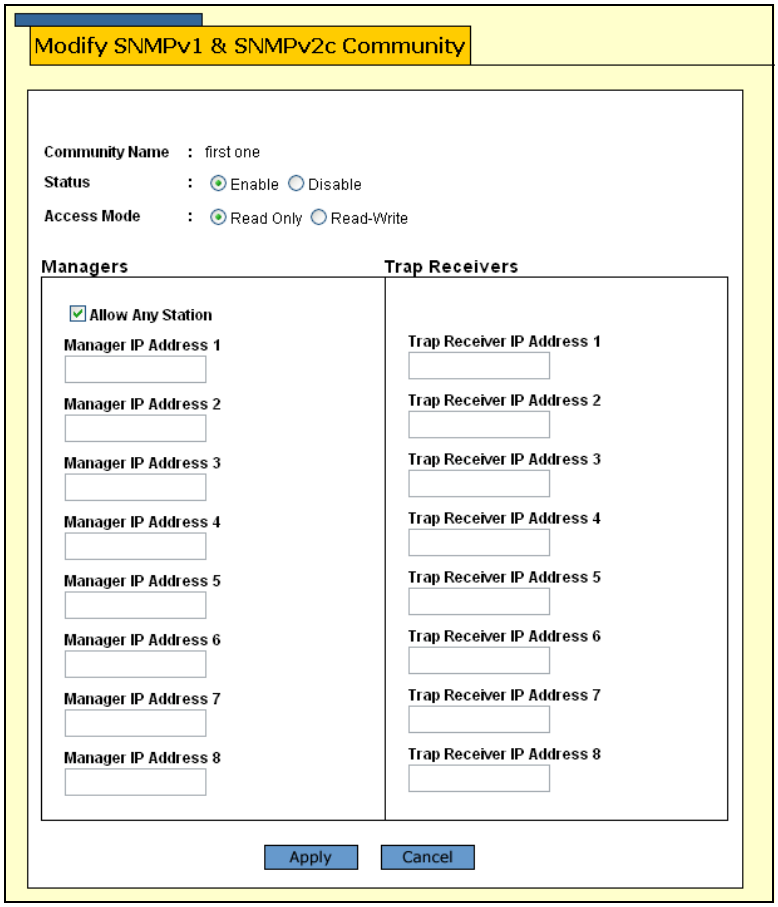
Modify SNMPv1 & SNMPv2c Community
Community Name : first one
Status : Enable Disable
Access Mode : Read Only Read-Write
Managers
Trap Receivers
Allow Any Station
Manager IP Address 1
Manager IP Address 2
Manager IP Address 3
Manager IP Address 4
Manager IP Address 5
Manager IP Address 6
Manager IP Address 7
Manager IP Address 8
Trap Receiver IP Address 1
Trap Receiver IP Address 2
Trap Receiver IP Address 3
Trap Receiver IP Address 4
Trap Receiver IP Address 5
Trap Receiver IP Address 6
Trap Receiver IP Address 7
Trap Receiver IP Address 8
Apply
Cancel

Figure 17. Modify SNMPv1 & SNMPv2c Community Page

6. Modify the following parameters:

Community Name
This field is not configurable from this page. It is the name of the SNMP community.

Status
Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode
Click Read Only to allow read access to the SNMP community. Click Read-Write to allow read-write access to the SNMP community.

Allow Any Station
Click this option to allow any SNMP manager to access the switch. When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address1 through **Manager IP Address 8**
Enter an IP Address of a switch that is permitted SNMP manager

access to the current switch. You can enter up to 8 Manager IP Addresses.

Trap Receiver IP Address 1 through **Trap Receiver IP Address 8** Use the above selections to specify the IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

7. Click **Apply**.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an SNMPv1 and SNMPv2c Community

To delete an existing SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14 on page 64.

4. In the SNMPv1 & SNMPv2c section, click **Configure**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 15 on page 66.

5. Click the button next to the community name to delete and click **Remove**.

   A warning message is displayed.

6. Click **OK**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the SNMPv1 and SNMPv2c Communities

To display the SNMPv1 and SNMPv2c communities, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab displayed by default, as shown in Figure 179 on page 436.

3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 18.

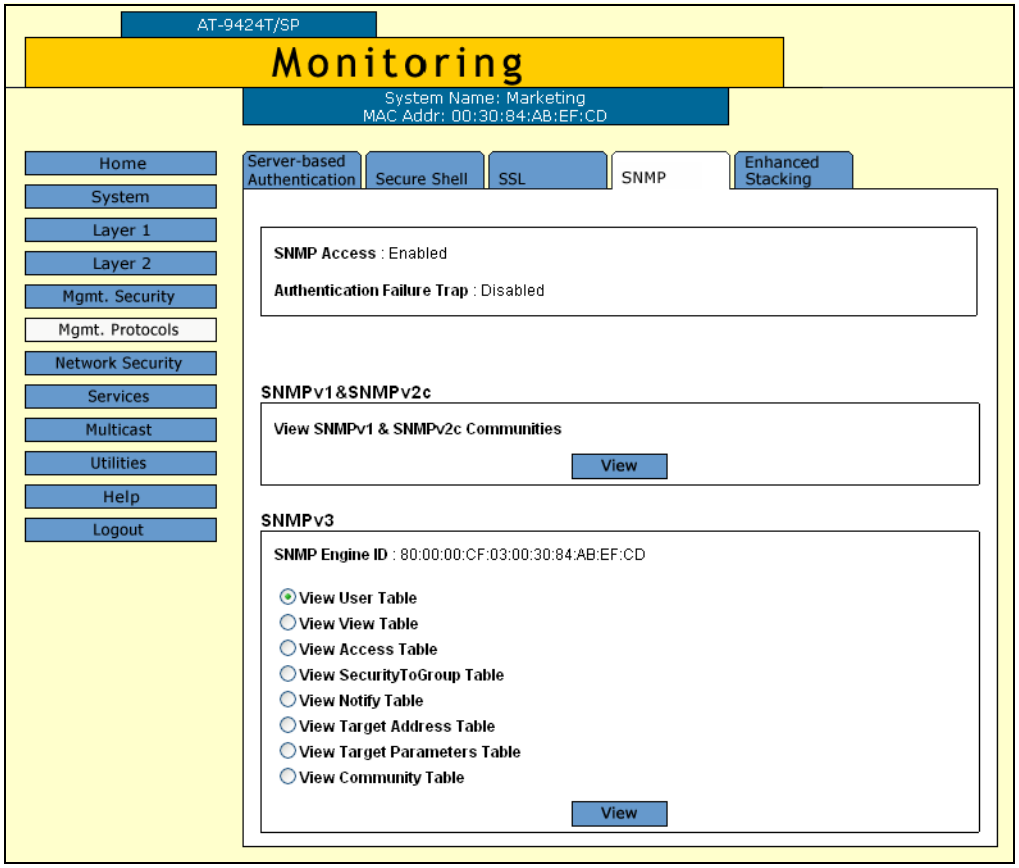

Figure 18. SNMP Tab (Monitoring)

4. In the SNMPv1 & SNMPv2c section, click **View**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 19.

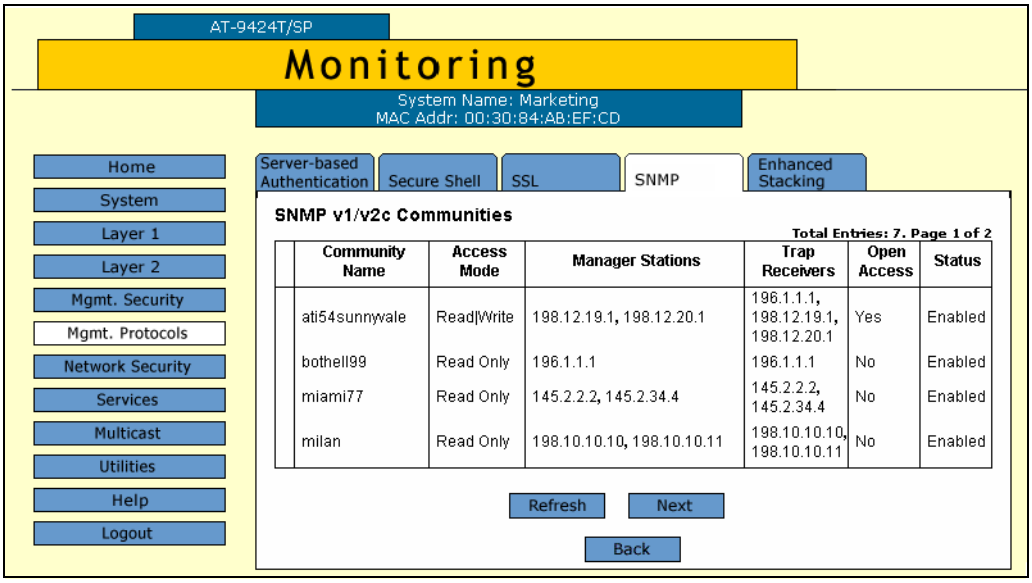

Figure 19. SNMPv1 & SNMPv2c Communities Tab (Monitoring)

The SNMPv1 & SNMPv2c Communities tab displays a table that contains the following columns of information:

Community Name
The SNMP community name.

Access Mode
The access mode for access to that community. The possible settings are Read Only and Read/Write.

Manager Stations
The IP addresses of the management stations that are allowed SNMP access to the switch using a community string. This only applies if the community string has a closed status.

Trap Receivers
The IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

Open Access
The status of access to the SNMP community by a management station, one of the following settings:

Yes - The community string has an open status, meaning that any management station can access the SNMP community.

No - The community string has an closed status, meaning that access to the SNMP community is only available to those management stations whose IP addresses are assigned to the community string.

Status
The community status, one of the following settings:

Enabled - The community is enabled.

Disabled - The community is disabled.

Chapter 5

Port Parameters

This chapter explains how to view and change the parameter settings for the individual ports on a switch. Examples of the parameters that you can adjust include port speed and duplex mode.

This chapter contains the following procedures:

- ❒ “Configuring Port Parameters” on page 78
- ❒ “Displaying Port Status” on page 85
- ❒ “Displaying Port Statistics” on page 89
- ❒ “Resetting a Port to the Default Settings” on page 92

Note
For further information about port parameters, refer to Chapter 6, “Port Parameters,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring Port Parameters

To configure the parameter settings of a port on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 20.

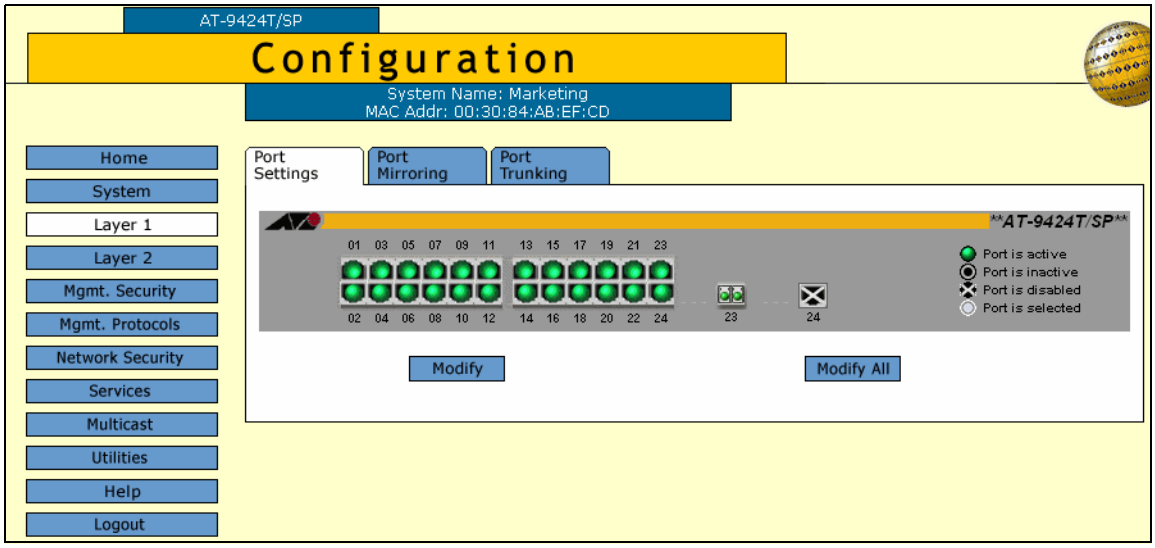

Figure 20. Port Settings Tab (Configuration)

3. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)

4. Click **Modify**. To configure all the ports, click **Modify All**.

> **Note**
> If you select Modify All, you cannot configure the port name or set the speed and duplex mode. The speed and duplex mode are set to autonegotiate.

The Port Configuration page is shown Figure 21.

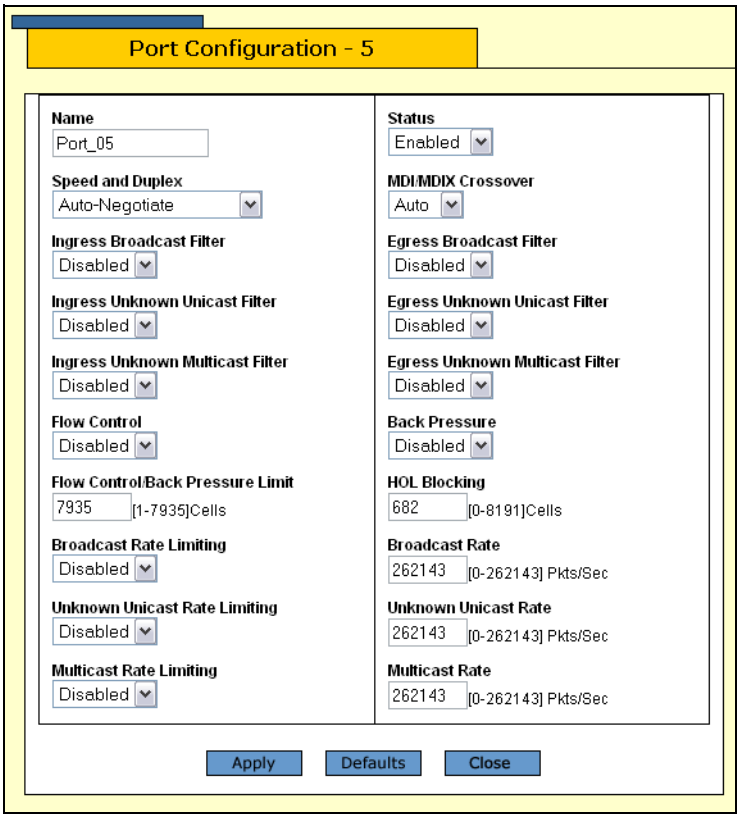

Figure 21. Port Configuration Page

5. Configure the following parameters as necessary.

   Name
   Use this selection to assign a name to a port, from 1 to 15 alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points. (You cannot assign a name when you are configuring more than one port.)

   Status
   Use this selection to enable or disable a port. When disabled, a port does not accept or forward frames.

   You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. After the problem has been fixed, you can enable the port again to resume normal operation.

   You might also want to disable a port that is not being used to secure it from unauthorized connections.

   The possible settings are:

Enabled - The port receives and forwards packets. This is the default setting.

Disabled - The port does not receive or forward packets.

Speed and Duplex
You use this selection to configure a port for Auto-Negotiation or to manually set a port's speed and duplex mode.

If you select Auto-Negotiate for Auto-Negotiation, which is the default setting, the switch sets both speed and duplex mode for the port automatically.

Note the following about the operation of Auto-Negotiation on a switch port:

- In order for a switch port to successfully autonegotiate its duplex mode with an end node, the end node should also be using Auto-Negotiation. Otherwise, a duplex mode mismatch can occur. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This results in a mismatch if the end node is operating at a fixed duplex mode of full-duplex.

  To avoid this problem, when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

- If you disable Auto-Negotiation on a twisted pair port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. If you disable Auto-Negotiation and set a port's speed and duplex mode manually, you might also need to set the port's MDI/MDI-X setting as well.

Auto-Negotiate: The port autonegotiates both speed and duplex mode. This is the default.

To manually set the speed and duplex mode of a port, select one of the following:

10Mbps - Half Duplex

10Mbps - Full Duplex

100Mbps - Half Duplex

100Mbps - Full Duplex

1Gb - Full Duplex (Applicable only to 1000Base SFP and GBIC modules.)

Note
A 10/100/1000Base-T twisted pair port can operate at 1000 Mbps only when set to Auto-Negotiation. You cannot manually configure a 10/100/1000Base-T twisted pair port to 1000 Mbps.

MDI/MDIX Crossover
The wiring configuration of a twisted pair port. This setting does not apply to fiber optic ports. The possible settings are:

Auto - The port automatically configures itself as MDI or MDIX, depending upon the end node. This is the default. This setting is only available when a port's speed and duplex mode are set through Auto-Negotiation.

MDI - The port uses straight through cable.

MDIX - The port uses a crossover cable.

Ingress Broadcast Filter
Use this parameter to configure a port to forward or discard ingress broadcast packets. The possible settings are:

Enabled - The port discards ingress broadcast packets.

Disabled - The port forwards ingress broadcast packets. This is the default setting.

Egress Broadcast Filter
Use this parameter to configure a port to forward or discard broadcast packets. The possible settings are:

Enabled - The port discards egress broadcast packets.

Disabled - The port forwards egress broadcast packets. This is the default setting.

For further information about filters, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Ingress Unknown Unicast Filter
Use this parameter to configure a port to forward or discard ingress unknown unicast packets. The possible settings are:

Enabled - The port discards ingress unknown unicast packets.

Disabled - The port forwards ingress unknown unicast packets. This is the default setting.

Egress Unknown Unicast Filter
Use this parameter to configure a port to forward or discard egress unknown unicast packets. The possible settings are:

Enabled - The port discards egress unknown unicast packets.

Disabled - The port forwards egress unknown unicast packets. This is the default setting.

Ingress Unknown Multicast Filter
Use this parameter to configure a port to forward or discard ingress unknown multicast packets. The possible settings are:

Enabled - The port discards ingress unknown multicast packets.

Disabled - The port forwards ingress unknown multicast packets. This is the default setting.

Egress Unknown Multicast Filter
Use this parameter to configure a port to forward or discard egress unknown multicast packets. The possible settings are:

Enabled - The port discards egress unknown multicast packets.

Disabled - The port forwards egress unknown multicast packets. This is the default setting.

Flow Control
Sets flow control on a port. This option only applies to ports operating in full-duplex mode. A switch port uses back pressure to control the flow of ingress packets. The switch sends a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time. The possible settings are:

Auto - The port uses flow control if it detects that the end node is using it.

Disabled - No flow control on the port. This is the default.

Enabled - Flow control is activated.

For further information about flow control, refer to Chapter 6, “Port Parameters,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Back Pressure
Use this parameter to set back pressure on a port. This option only appears for ports operating in half-duplex mode. A switch port uses back pressure to control the flow of ingress packets. The possible settings are:

Enabled - Back pressure is enabled.

Disabled - Back pressure is disabled. This is the default.

For further information about back pressure, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Flow Control/Back Pressure Limit
Use this parameter to specify the maximum number of ingress packets that a port receives within a one second period before initiating flow control or back pressure.A cell equals 128 bytes. The range is 1 to 7935. The default is 7935 cells.

The following three parameters allow you to set rate limiting, the maximum number of ingress packets a port accepts each second. Packets exceeding the threshold are discarded.

HOL Blocking
HOL blocking sets a threshold on the utilization of a port's egress queue. When the threshold for a port is exceeded, the switch signals other ports to discard packets to the oversubscribed port. The possible settings are:

Enabled - HOL blocking prevention is activated.

Disabled - HOL blocking is inactivated on this port.

You also set the rate limit in number of cells. A cell is 128 bytes. The range is 1 to 8191. The default is 682. For more information about HOL blocking, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Broadcast Rate Limiting
Use this parameter to enable or disable ingress broadcast packet limits. The possible settings are:

Enabled - Broadcast packet ingress rate limiting is enabled.

Disabled - Broadcast packet ingress rate limiting is disabled. This is the default.

Broadcast Rate
Use this parameter to set the broadcast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Unknown Unicast Rate Limiting
Use this parameter to enable or disable ingress unknown unicast packet limits. The possible settings are:

Enabled - Unknown unicast packet ingress rate limiting is enabled.

Disabled - Unknown unicast packet ingress rate limiting is disabled. This is the default.

Unknown Unicast Rate
Use this parameter to set the unknown unicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Multicast Rate Limiting
Use this parameter to enable or disable ingress multicast packet limits. The possible settings are:

Enabled - Multicast packet ingress rate limiting is enabled.

Disabled - Multicast packet ingress rate limiting is disabled. This is the default.

Multicast Rate
Use this parameter to set the multicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

6. After you have made the desired changes, click **Apply**.

   The switch activates the parameter changes on the port.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying Port Status

To display the status of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 22.

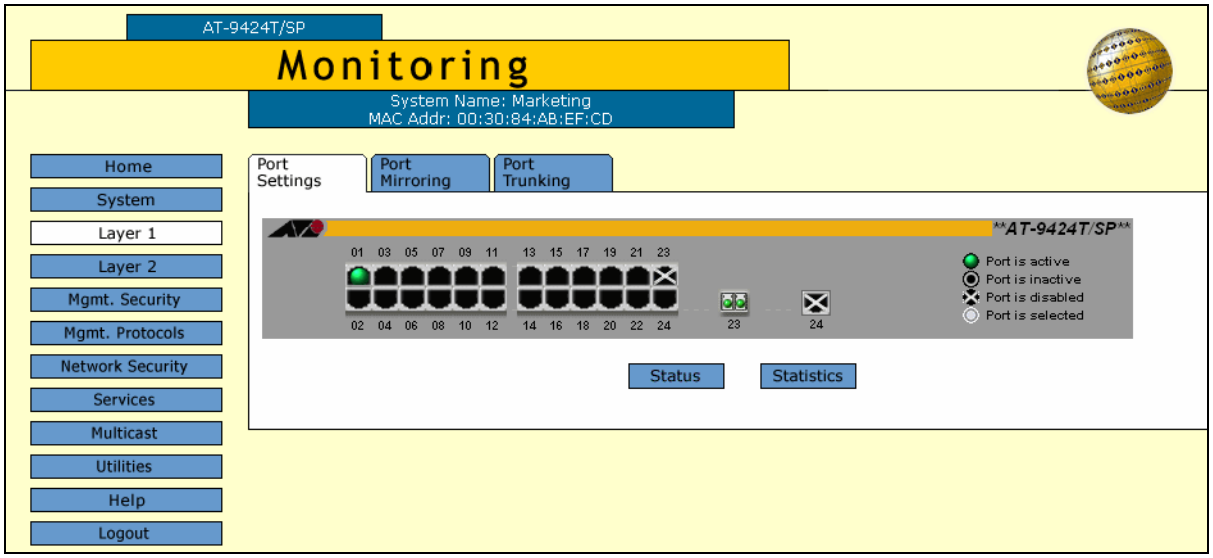

Figure 22. Port Settings Tab (Monitoring)

   The Port Settings tab displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

3. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)

4. Click **Status**.

The Port Status page is shown in Figure 23.

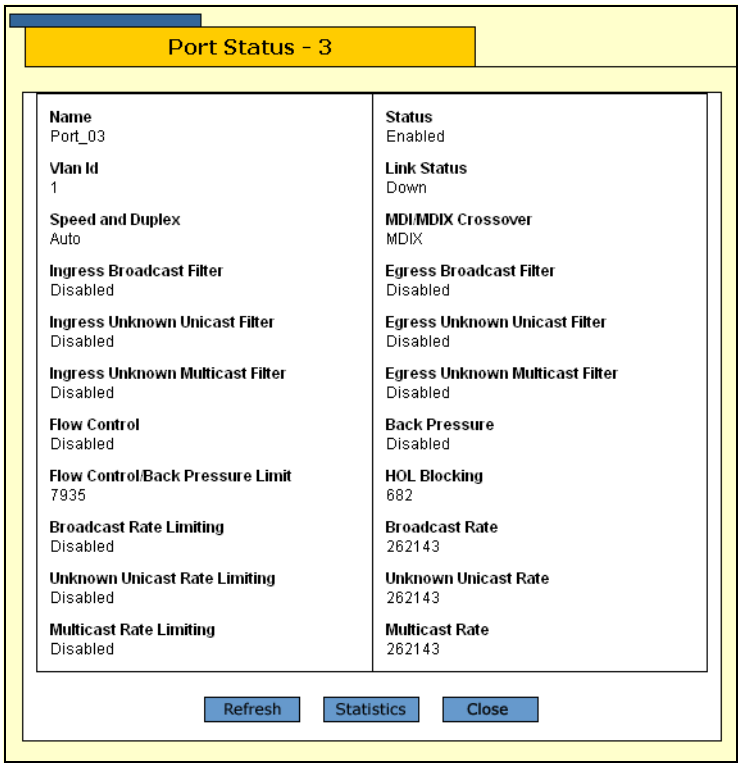

Figure 23. Port Status Page

The Port Status page displays the following information:

Name
The name of the port.

Status
The status of the port, enabled or disabled.

VLAN ID
The VLAN identifier (VID) of the VLAN in which the port is an untagged member.

Link Status
The status of the link between the port and the end node connected to the port, up or down.

Speed and Duplex
The speed and duplex mode.

MDI/X Crossover
The operating configuration of the port. The possible settings are MDI and MDI-X.

Ingress Broadcast Filter
Status of the filter on ingress broadcast packets.

Ingress Unknown Unicast Filter
Status of the filter on ingress unknown unicast packets.

Ingress Unknown Multicast Filter
Status of the filter on ingress unknown multicast packets.

Flow Control
Status of flow control, enabled or disabled.

Flow Control/Back Pressure Limit
The flow control/back pressure limit.

Broadcast Rate Limiting
The status of rate limiting on broadcast packets.

Unknown Unicast Rate Limiting
The status of rate limiting on broadcast packets.

Multicast Rate Limiting
The status of rate limiting on broadcast packets.

Status
The overall status of the port, enabled or disabled.

Egress Broadcast Filter
The status of the filter on egress broadcast packets.

Egress Unknown Unicast Filter
The status of the filter on egress unknown unicast packets.

Egress Unknown Multicast Filter
The status of the filter on egress unknown multicast packets.

Back Pressure
The status of back pressure on the port, enabled or disabled.

Flow Control/Back Pressure Limit
The flow control and back pressure limit.

HOL Blocking
The Head of Line Blocking setting.

Broadcast Rate Limiting
The status of broadcast rate limiting, enabled or disabled.

Broadcast Rate
The rate on broadcast packets.

Unknown Unicast Rate Limiting
The status of unknown unicast rate limiting, enabled or disabled.

Unknown Unicast Rate
The rate on unknown unicast packets.

Multicast Rate Limiting
The status of multicast rate limiting, enabled or disabled.

Multicast Rate
The rate on multicast packets.

Displaying Port Statistics

To display the statistics of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 22 on page 85

   The Port Setting tab displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

3. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)

4. Click **Statistics**.

   The Port Statistics page is shown in Figure 24.

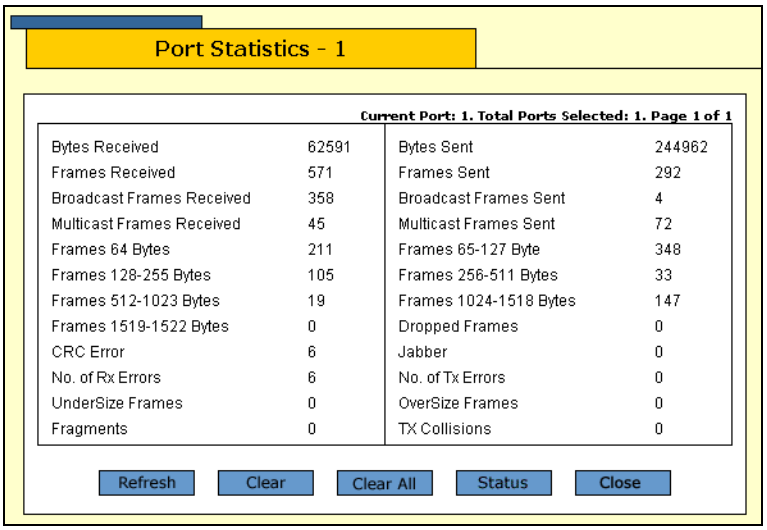

Figure 24. Port Statistics Page

The Port Statistics page displays a table that contains the following columns of information:

Bytes Received
Number of bytes received on the port.

Bytes Sent
Number of bytes transmitted from the port.

Frames Received
Number of frames received on the port.

Frames Sent
Number of frames transmitted from the port.

Broadcast Frames Received
Number of broadcast frames received on the port.

Broadcast Frames Sent
Number of broadcast frames transmitted from the port.

Multicast Frames Received
Number of multicast frames received on the port.

Multicast Frames Sent
Number of multicast frames transmitted from the port.

Frames 64 Bytes
Frames 65 - 127 Bytes
Frames 128 - 255 Bytes
Frames 256 - 511 Bytes
Frames 512 - 1023 Bytes
Frames 1024 - 1518 Bytes
Frames 1519 - 1522
Number of frames transmitted from the port, grouped by size.

CRC Error
Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Jabber
Number of occurrences of corrupted data or useless signals appearing on the port.

No. of Rx Errors
Total number of frames received on the port containing errors.

Undersize Frames
Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Frames
Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received on the port.

TXCollisions
Number of transmit collisions.

5. To clear all the counters for the selected port, click **Clear**. To clear the counters for all ports on the switch, click **Clear All**.

Resetting a Port to the Default Settings

To reset a port to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 20 on page 78.

3. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)

4. Click **Modify**. To configure all of the ports, click **Modify All**.

   The Port Configuration page is displayed, as shown Figure 21 on page 79.

5. Click **Defaults**.

   The port(s) are returned to the default settings.

Chapter 6

MAC Address Table

This chapter contains instructions on how to add and view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

- ❒ “Adding Static Unicast and Multicast MAC Addresses” on page 94
- ❒ “Deleting Unicast and Multicast MAC Addresses” on page 96
- ❒ “Deleting All Dynamic MAC Addresses” on page 97
- ❒ “Displaying the MAC Address Tables” on page 98
- ❒ “Changing the Aging Time” on page 101

Note
For background information on MAC address tables, refer to Chapter 7, “MAC Address Table,” in the *AT-S63 Management Software Menus Interface User’s Guide.*

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for assigning a static unicast or multicast address to a port on the switch. You can assign up to 255 static MAC addresses per port.

To add a static address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25.

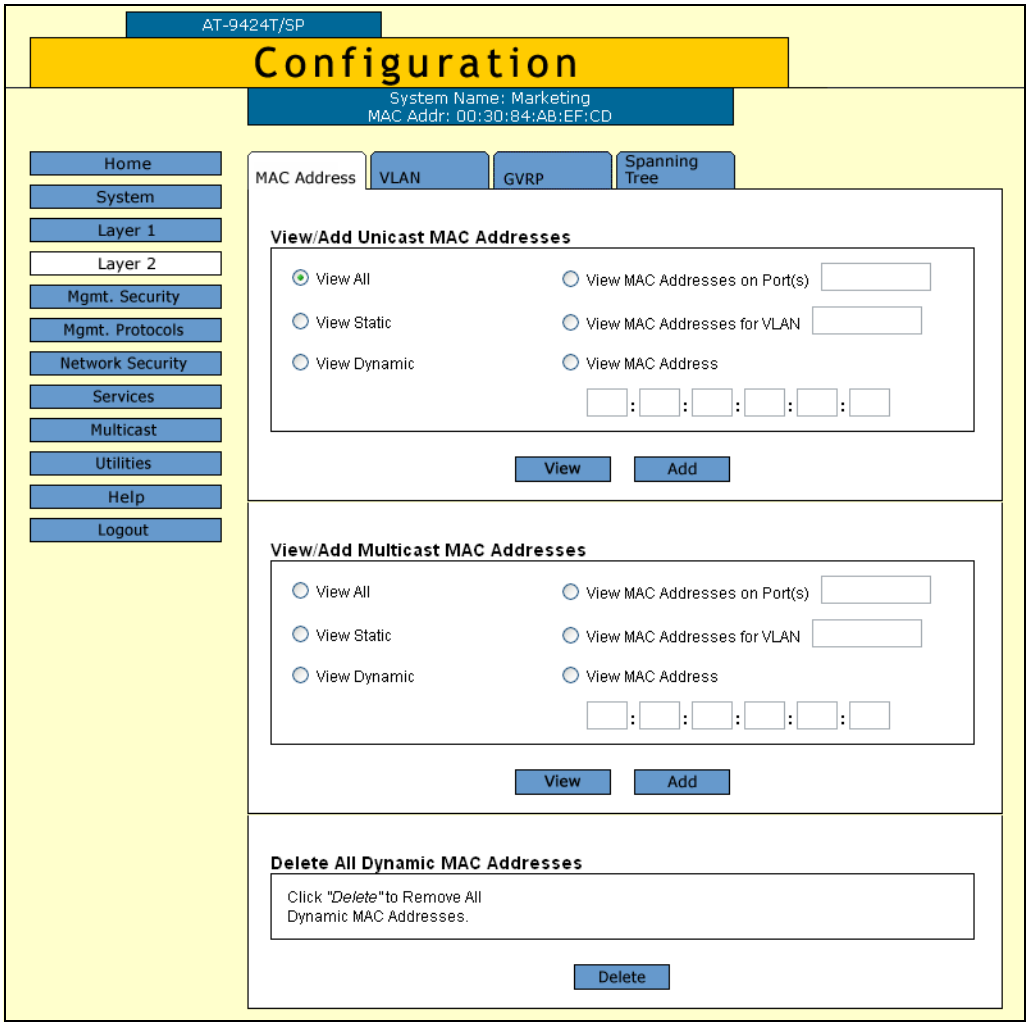

Figure 25. MAC Address Tab (Configuration)

3. To add a static unicast address, in the View/Add Unicast MAC Addresses section, click **Add**. To add a static multicast address, in the View/Add Multicast MAC Addresses section, click **Add**.

   The Add MAC Address page is shown in Figure 26.

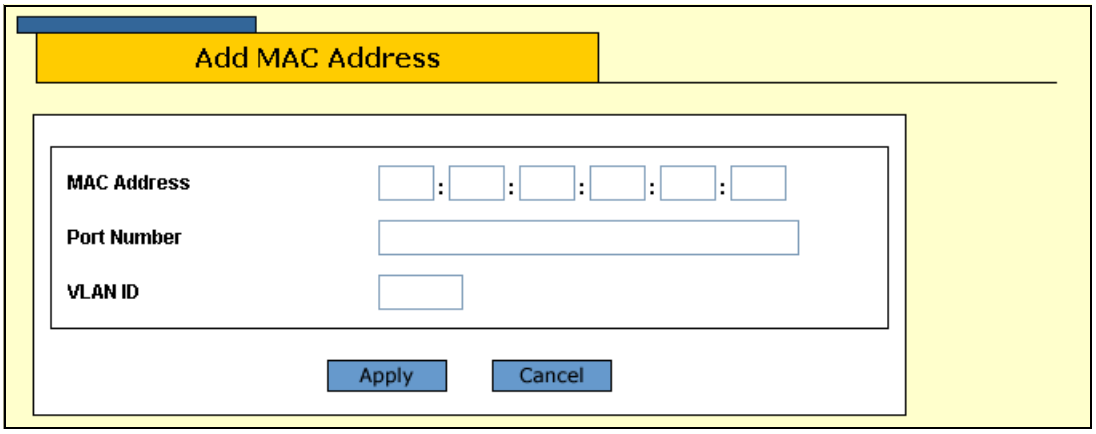

Figure 26. Add MAC Address Page

4. Configure the following parameters as necessary.

   MAC Address
   The new static unicast or multicast MAC address.

   Port Number
   The number of the port on the switch where you want to assign the static address. If you are adding a static unicast address, you can enter only one port.

   If you are entering a static multicast address, you must specify the port when the multicast application is located as well as the ports where the host nodes are connected. Assigning the address only to the port where the multicast application is located results in the failure of the multicast packets to be properly forwarded to the host nodes. You can specify the ports individually (e.g., 1,4,5), as a range (e.g., 11-14) or both (e.g., 15-17,22,24).

   VLAN ID
   The VLAN ID where the port is a member.

5. Click **Apply**.

6. Repeat this procedure to add other static addresses to the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting Unicast and Multicast MAC Addresses

To delete a static or dynamic unicast or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Display the MAC addresses on the switch by selecting one of the options.

   For detailed instructions, refer to “Displaying the MAC Address Tables” on page 98.

4. Click the button next to the MAC address that you want to delete from the switch.

5. Click **Remove**.

   Note
   You cannot delete a switch’s MAC address, an STP BPDU MAC address, or a broadcast address.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting All Dynamic MAC Addresses

To delete all the dynamic MAC addresses, unicast or multicast, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. In the Delete All Dynamic MAC Addresses section, click **Delete**.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the MAC Address Tables

To view the MAC address table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 27.

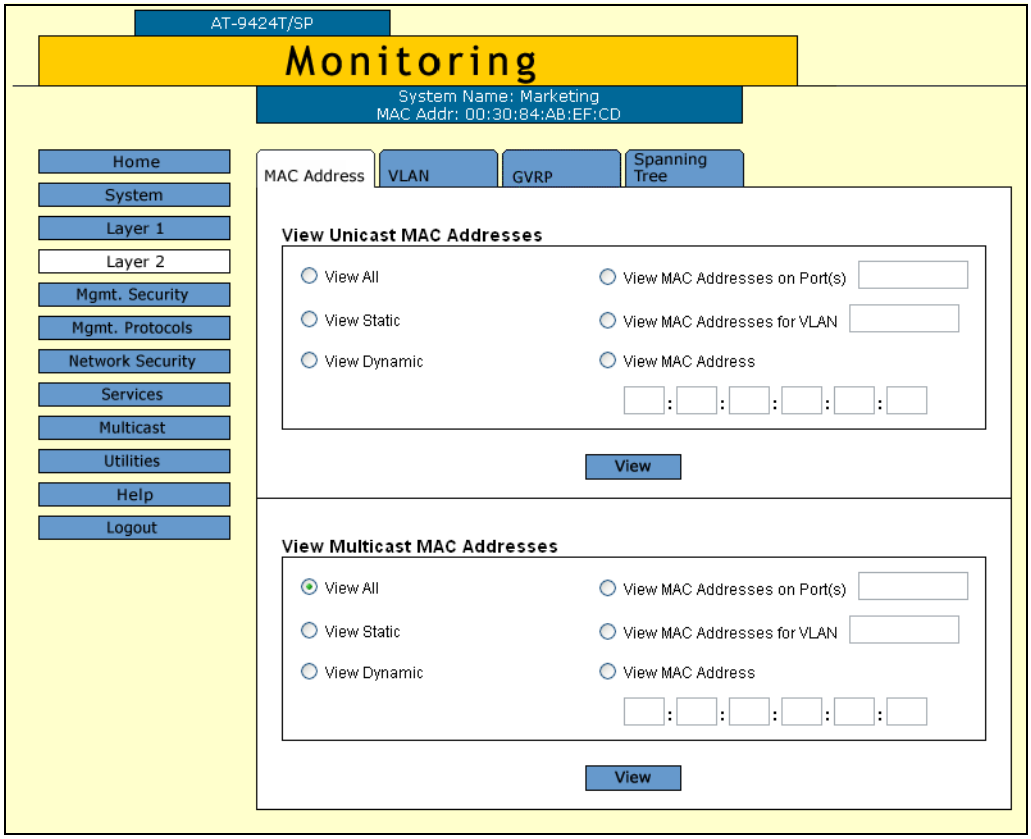

Figure 27. MAC Address Tab (Monitoring)

The tab contains two sections. The View Unicast MAC Addresses section displays unicast addresses. The View Multicast MAC Addresses section displays multicast addresses. The options function the same in both sections, and are described below. You can select only one option at a time.

View All
Displays all dynamic addresses learned on the ports of the switch and all static addresses that have been assigned to the ports.

View Static
Displays just the static addresses assigned to the ports on the switch.

View Dynamic
Displays only the dynamic addresses learned on the ports on the switch.

View MAC Addresses on Port
Displays the dynamic and static MAC addresses of a particular port. You can specify more than one port at a time.

View MAC Addresses for VLAN
Displays the static and dynamic addresses learned on the tagged and untagged ports of a specific VLAN. You specify the VLAN by entering the VLAN ID number. You can specify only one VLAN at a time.

View MAC Address
Displays the port number on which a MAC address was assigned or learned.

In some situations, you might want to know on which port a particular MAC address was learned. You could display the MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The View MAC Address option allows you to specify the MAC address and let the AT-S63 management software automatically locate the port on the switch where the device is connected.

3. After you select an option, click **View.**

Figure 28 shows an example of viewing all unicast MAC addresses.

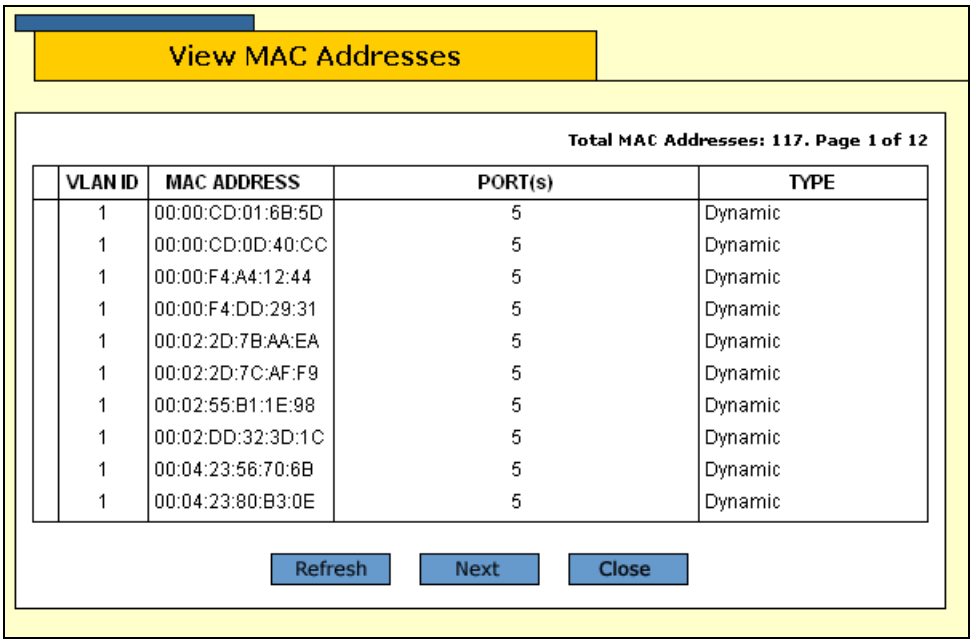

Figure 28. View MAC Addresses Page

The View MAC Addresses page displays a table that contains the following columns of information:

VLAN ID
The ID number of the VLAN where the port is a member.

MAC Address
The static or dynamic unicast MAC address.

Port(s)
The port on which the address was learned or assigned. The MAC address with port “CPU” is the address of the switch.

Type
The type of the address: static or dynamic.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To configure the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. In the Configuration section, for the MAC Address Aging Time, enter a new value in seconds. The range is 0 to 1048575 seconds. The default is 300 seconds (5 minutes). The value 0 disables the aging timer. If the aging timer is disabled, inactive dynamic addresses are not deleted from the table and the switch stops learning new addresses after the table reaches maximum capacity.

3. Click **Apply**.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Chapter 7

Static Port Trunks

This chapter contains the procedure for creating, modifying, or deleting a static port trunk. The sections in this chapter are:

- “Creating a Static Port Trunk” on page 104
- “Modifying a Static Port Trunk” on page 107
- “Deleting a Port Trunk” on page 109
- “Displaying the Port Trunks” on page 110

Note
For background information on static port trunking, refer to Chapter 8, “Static and LACP Port Trunks,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a Static Port Trunk

Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely effect the operation of your network.

Note

Before creating a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port that will be a part of the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the AT-S63 management software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

To create a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 29 and displays any existing trunks in a table.

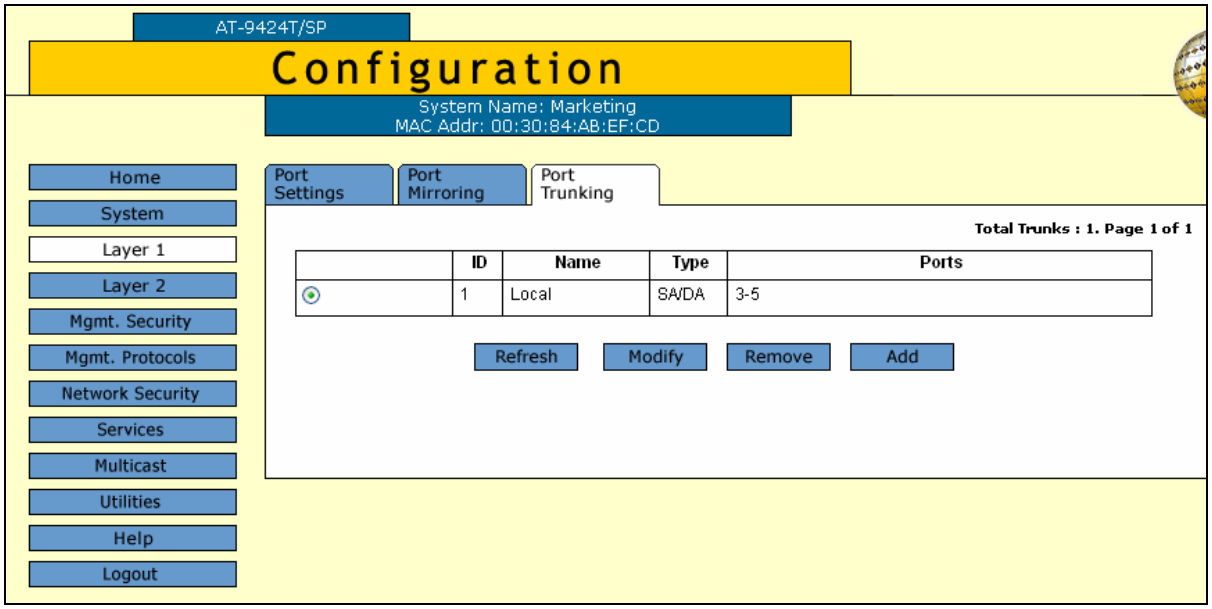

Figure 29. Port Trunking Tab (Configuration)

4. Click **Add**.

   The Add New Trunk page is shown in Figure 30.

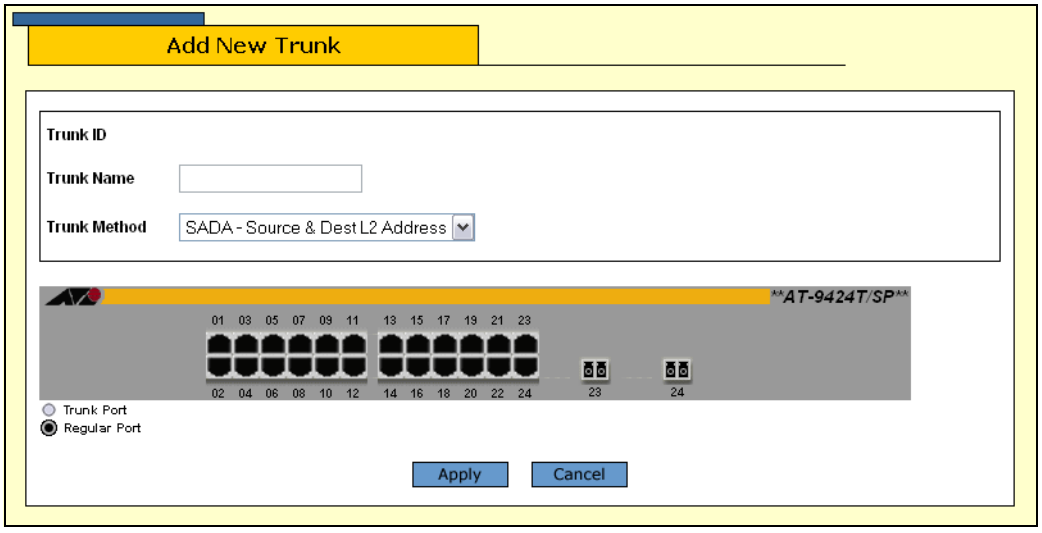

Figure 30. Add New Trunk Page

5. Configure the following parameters as necessary.

   Trunk Name
   The name for the port trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and

exclamation points, are allowed. Each trunk must be given a unique name.

Trunk Method
Select a load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

6. Click the ports that are to make up the static port trunk. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.

   Note
   All ports in a trunk must operate at the same speed. When you include port 23R or 24R on an AT-9424 switch in a trunk and the port transitions to redundant uplink status, the port speed is automatically adjusted to 1000 Mbps. If the other ports in the trunk are operating at a different speed, port trunking may be unpredictable. Because of these port speed variables, Allied Telesyn suggests that you not include port 23R or 24R in a port trunk.

7. Click **Apply**.

   The new port trunk is now active on the switch.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

9. Configure the ports on the remote switch for port trunking.

10. Connect the cables to the ports of the trunk on the switch.

    The port trunk is ready for network operations.

Modifying a Static Port Trunk

This section contains the procedure for modifying a static port trunk on the switch. You can change the name of a trunk and the ports that constitute the trunk. You cannot change the load distribute method. Be sure to review the guidelines in Chapter 8, "Static and Dynamic Port Trunking," in the *AT-S63 Management Software Menus Interface User's Guide* before you perform the procedure:

Caution
If you are adding or removing ports from the trunk, you should disconnect all data cables from the ports of the trunk on the switch before performing the procedure. Adding or removing ports from a port trunk without first disconnecting the cables may result in loops in your network topology. Loops can produce broadcast storms and poor network performance.

Note the following before performing this procedure:

- If you are adding a port and the port will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you should check to see if its settings are appropriate prior to adding it.
- If you are adding a port and the port will not be the lowest numbered port in the trunk, its settings will be changed to match the settings of the existing ports in the trunk.
- If you are adding a port to a trunk, check to be sure that the new port is an untagged member of the same VLAN as the other trunk ports. A trunk cannot contain ports that are untagged members of different VLANs.
- You cannot change the load distribution method of a static port trunk from the web browser manager interface, but you can from the menus or command line interface.

To modify a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 29 on page 105.

4. Click the button next to the port trunk you want to modify and click **Modify**.

   The Modify Trunk page is shown in Figure 31.

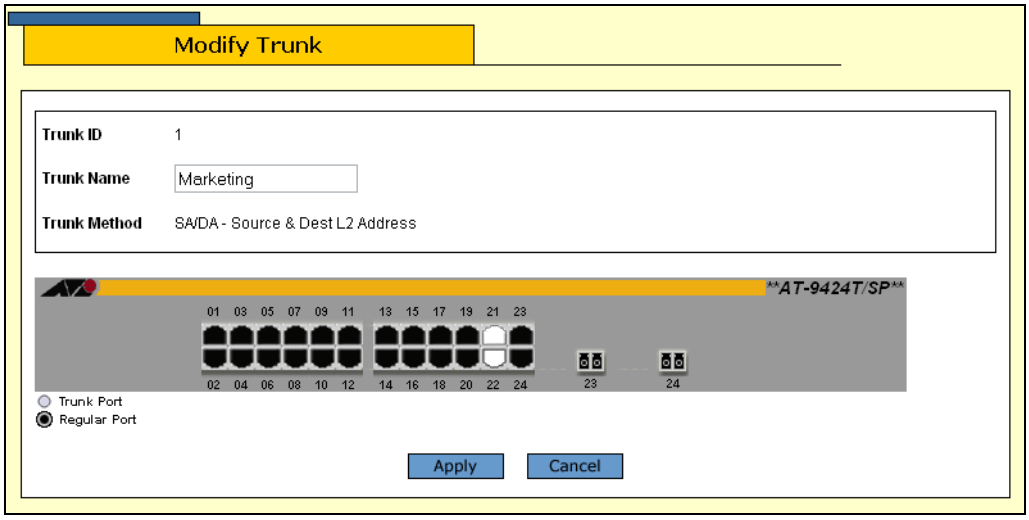

Figure 31. Modify Trunk Page

Note
You cannot change the Trunk ID number or the load distribution method of a static port trunk from the web browser interface.

5. Configure the following parameter as necessary.

   Trunk Name
   The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.

6. To add or remove ports from a trunk, click the ports in the graphical image of the switch. A selected port changes to white. An unselected port is black. A static port trunk can contain up to eight ports.

7. Click **Apply**. Changes to a port trunk are activated on the switch.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

9. Reconnect the cables to the ports of the trunk.

Deleting a Port Trunk

> **Caution**
> Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 29 on page 105.

4. Click the button next to the port trunk you want to delete and click **Remove**.

   The port trunk is deleted from the switch.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port Trunks

To display the port trunks, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 22 on page 85.

3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 32.

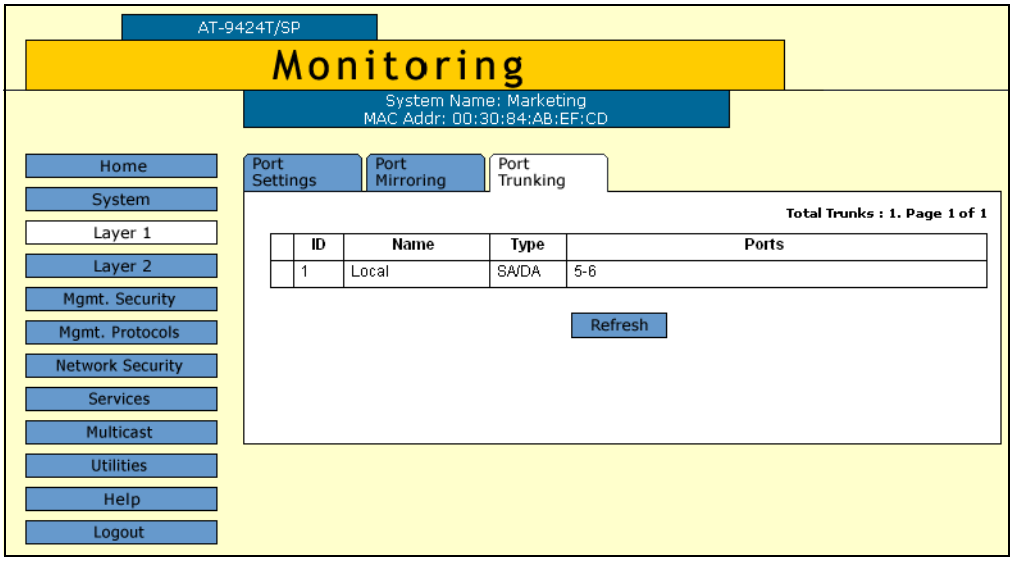

Figure 32. Port Trunking Tab (Monitoring)

The Port Trunking tab displays a table that contains the following columns of information:

ID
The ID number of the trunk.

Name
The name of the trunk.

Type
The load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

Ports
The ports of the trunk.

Chapter 8

Port Mirroring

This chapter contains the procedures for creating or deleting a port mirror. The sections in the chapter include:

- ❒ “Creating a Port Mirror” on page 114
- ❒ “Modifying a Port Mirror” on page 117
- ❒ “Disabling a Port Mirror” on page 118
- ❒ “Deleting a Port Mirror” on page 119
- ❒ “Displaying the Port Mirror” on page 120

Note
For background information on port mirroring, refer to Chapter 9, “Port Mirroring,” in the *AT-S63 Management Software Menus Interface User’s Guide.*

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 33 with any configured mirror.

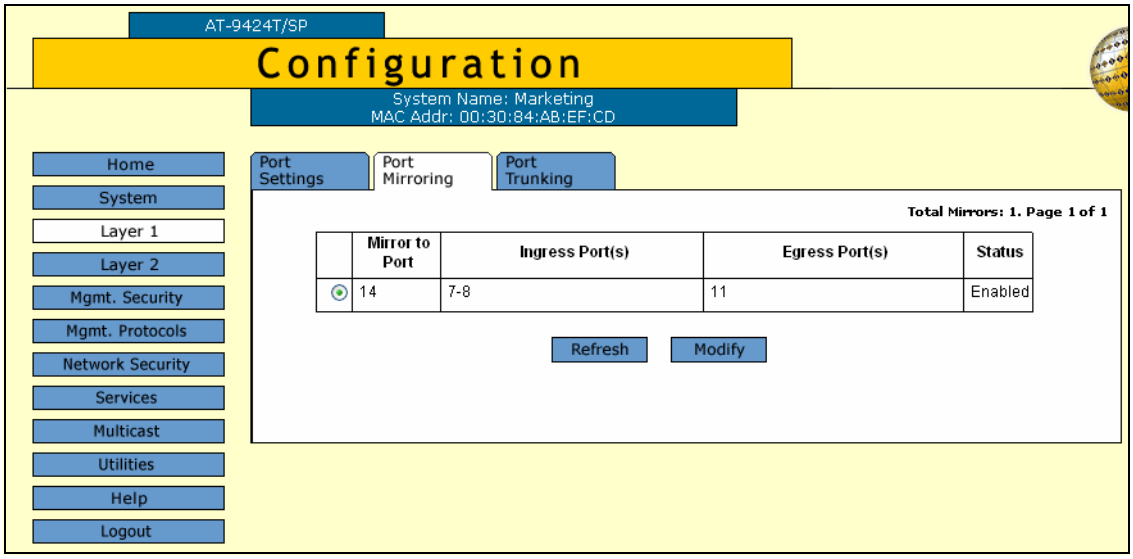

Figure 33. Port Mirroring Tab (Configuration)

   This tab displays any port mirror already existing on the switch. If the Mirror to Port column contains a 0 (zero), there is no port mirror.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 34.

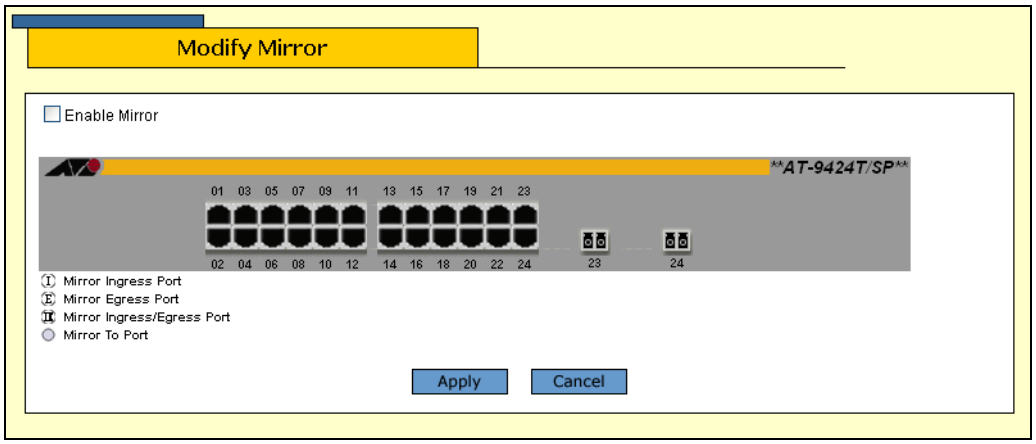

Figure 34. Modify Mirror Page

5. Click the ports of the port mirror. Clicking a port toggles it through the possible settings, which are as follows:

The destination (mirror) port. There can be only one destination port.

A source port. The port's ingress traffic is mirrored to the destination port.

A source port. The port's egress traffic is mirrored to the destination port.

A source port. The port's ingress and egress traffic is mirrored to the destination port.

Not part of a port mirror.

You can mirror one port, a few ports, or all of the ports on the switch, with the exception, of course, of the destination port.

Figure 35 shows an example of the Modify Mirror page configured for a port mirror. The egress traffic on ports 11 and 12 is being mirrored to the destination port 5.

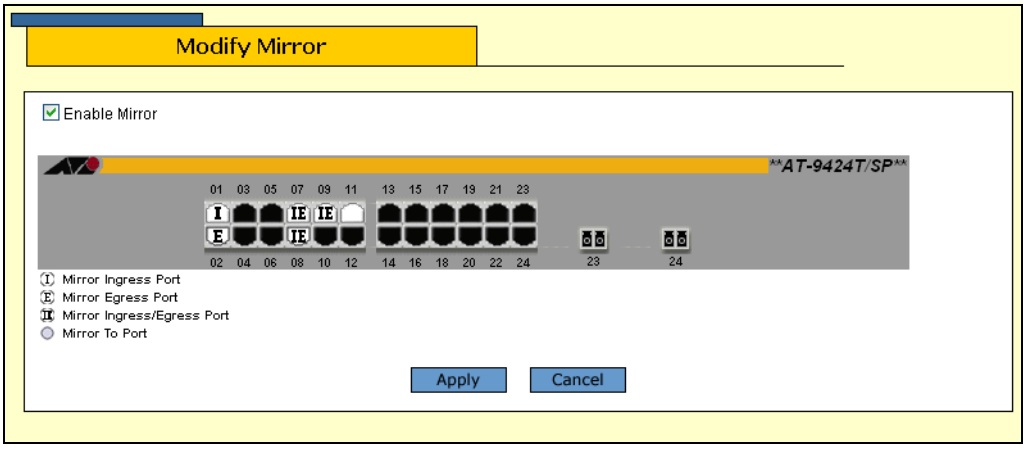

Figure 35. Example of a Modify Mirror Page

6. After selecting the destination and source ports, click the **Enable Mirror** check box.

7. Click **Apply**.

   The port mirror is now active on the switch. You can connect a data analyzer to the destination port to monitor the traffic on the source ports.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Port Mirror

To modify a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 33 on page 114.

4. Click **Modify**.

   The Modify Mirror page is shown in Figure 34 on page 115.

5. Click the ports of the port mirror to change its type. Clicking a port toggles it through the possible settings, which are as follows:

   The destination (mirror) port. There can be only one destination port.

   A source port. The port's ingress traffic is mirrored to the destination port.

   A source port. The port's egress traffic is mirrored to the destination port.

   A source port. The port's ingress and egress traffic is mirrored to the destination port.

   Not part of a port mirror.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Disabling a Port Mirror

To disable a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 33 on page 114.

4. Click **Modify**.

   The Modify Mirror page is shown in Figure 34 on page 115.

5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Port Mirror

To delete a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 20 on page 78.

3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 33 on page 114.

4. Click **Modify**.

   The Modify Mirror page is shown in Figure 34 on page 115.

5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.

6. Click **Apply**.

7. Click the destination port, which is white, so that it is black.

8. Click **Apply**.

9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port Mirror

To display the port mirror, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 22 on page 85.

3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 36.

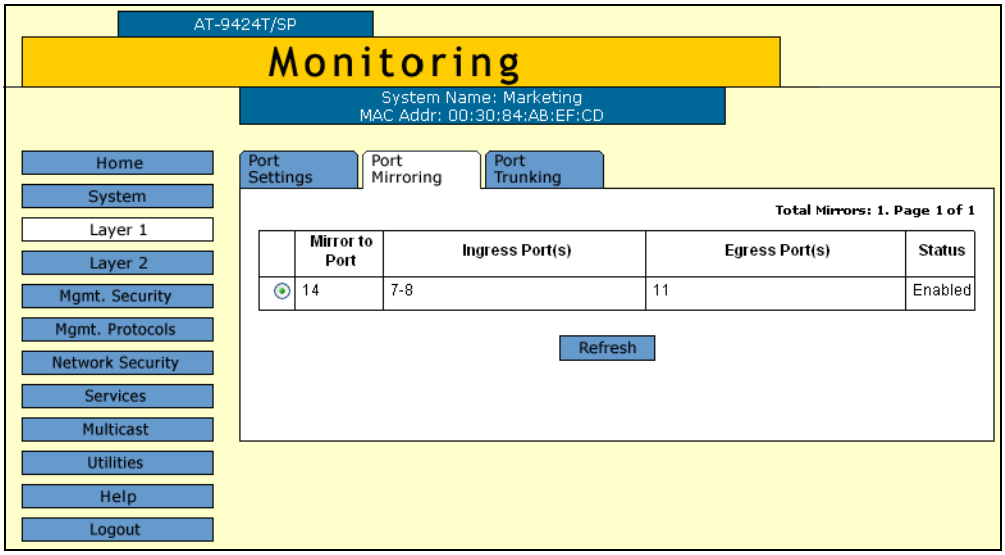

Figure 36. Port Mirroring Tab (Monitoring)

The Port Mirroring tab displays a table that contains the following columns of information:

Mirror to Port
The destination port to which the traffic is copied and where the network analyzer is located.

Ingress Port(s)
The source ports whose ingress traffic is mirrored to the destination port.

Egress Port(s)
The source ports whose egress traffic is mirrored to the destination port.

Status
The status of the mirroring feature. The possible settings are:

Enabled - Traffic is being copied to the destination port.

Disabled - No traffic is being mirrored.

Section II

Advanced Operations

The chapters in this section contain the procedures for advanced switch setup using the AT-S63 management software. The chapters include:

- Chapter 9, “File System” on page 125
- Chapter 10, “File Downloads and Uploads” on page 133
- Chapter 11, “Event Logs and Syslog Servers” on page 141
- Chapter 12, “Classifiers” on page 159
- Chapter 13, “Access Control Lists” on page 171
- Chapter 14, “Class of Service” on page 181
- Chapter 15, “Quality of Service” on page 191
- Chapter 16, “Denial of Service Defense” on page 213
- Chapter 17, “IGMP Snooping” on page 219

Chapter 9

File System

This chapter contains procedures for working with the file system and contains the following sections:

- ❒ “Listing the Files in Flash Memory or on a Compact Flash Card” on page 126
- ❒ “Selecting an Active Boot Configuration File” on page 130

Note
For background information on the file system, refer to Chapter 11, “File System,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Listing the Files in Flash Memory or on a Compact Flash Card

This procedure displays the files stored in flash memory as well as on a compact flash card for those AT-9400 Series switches that feature a flash card slot.

> **Note**
> You cannot copy, rename, or delete files from a web browser management session. Those tasks must be performed from a local, Telnet, or SSH session.

To display a list of the system files stored in flash memory as well as on a compact flash card (if the switch supports this and a compact flash card is inserted in the slot), perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab displayed by default, as shown in Figure 10 on page 53.

3. Select the **File System** tab.

The FIle System tab for an AT-9400 Series switch with a flash memory card drive is shown in Figure 37.

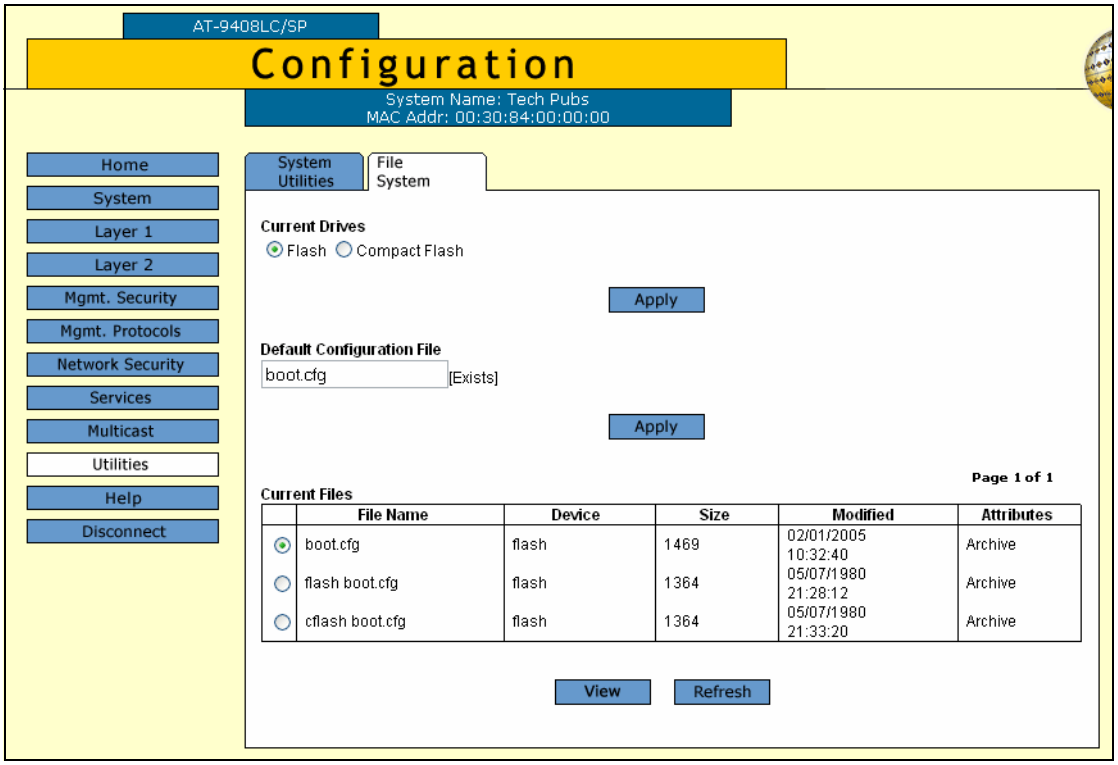

Figure 37. File System Tab (Configuration)

The information in the tab is defined below:

Current Drives
Specifies the location of the file system. An AT-9400 Series switch that does not feature a flash card slot has just one selection, Flash, which represents the flash memory in the switch. An AT-9400 Series switch that has a flash card slot has two selections, Flash and Flash Card. The example tab in Figure 37 is from a switch that has a flash card slot.

Default Configuration File
Specifies the filename of the active configuration file. The switch uses this file to configure its operating parameters when it is reset or power cycled. The active boot file is also the file that is updated when you select the Save Config option.

The columns in the List Files table are described below. This information is for viewing purposes only. If your unit has a compact flash card slot, the switch, by default, displays the files in flash memory. To view the files on a card, go to step 4.

File Name
Name of the system file.

Device
The device type, either “flash” for flash memory or “cflash” for compact flash card.

Size
Size of the file, in bytes.

Modified
The time the file was created or last modified, in the following date and time format: month/day/year hours:minutes:seconds.

Attributes
The file type, one of the following:

- Normal
- Read Only
- Hidden
- System
- Volume
- Directory
- Archive
- Invalid

4. To view the files on a compact flash card, insert the card into the slot on the switch, select **Compact Flash** under Current Drivers, and click **Apply**.

5. To view the contents of a configuration file, in the Current Files section click a file and click **View**. You can view one file at a time.

The Viewing File page for a portion of a configuration file is shown in Figure 38.

.

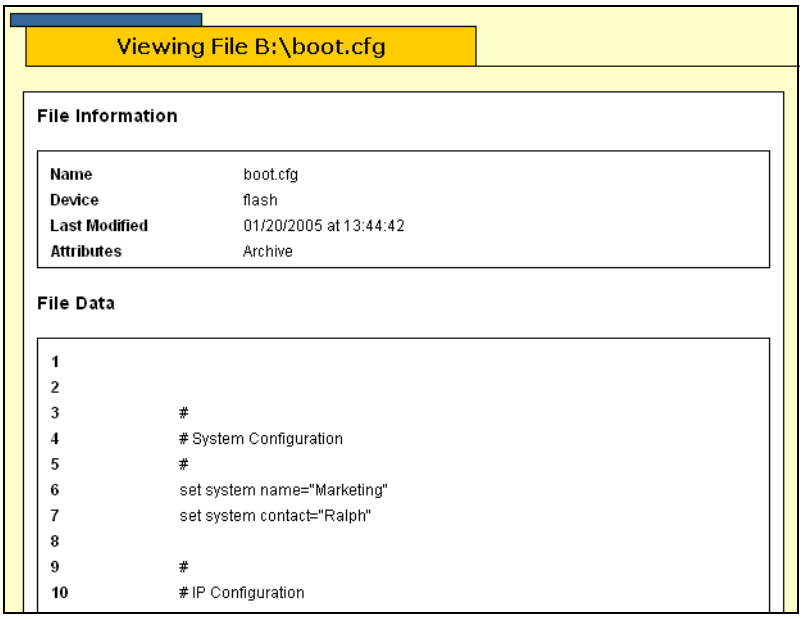

Figure 38. List Files Page

Selecting an Active Boot Configuration File

This procedure changes the active boot configuration file on the switch. The switch uses the active boot configuration file to configure its operating parameters whenever it is reset or power cycled. The switch also updates the active boot file whenever you select the Save Config option.

Note the following before performing this procedure:

- You cannot create a new configuration file from a web browser management session. That task must be performed from a local, Telnet, or SSH session using the menus or command line interface.
- The configuration file must already exist in the switch's file system or on a flash memory card, for those switches that support a flash card. To view the switch's configuration files, see "Listing the Files in Flash Memory or on a Compact Flash Card" on page 126. Configuration files have a ".cfg" extension.
- Specifying a new active boot configuration file does not change the current operating configuration of the switch. To reconfigure the switch in accordance to the configuration in a newly assigned active boot configuration file, reset or power cycle the switch at the end of the procedure.
- Selecting Save Config after changing the active configuration file overwrites the settings in the file with the current operating settings of the switch.
- You can specify a configuration file on a flash memory card for those systems that support a flash card. However, the switch does not copy the configuration file to its file system. Instead, it uses and updates the file directly on the card. If at some point you remove the card, the switch does not allow you to save any further configuration changes until you reinsert the flash card or specify another active boot configuration file. Additionally, if you reset the switch after removing a flash card that contains a switch's active boot configuration file, the management software uses the switch's default settings.

To change the switch's active configuration file, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab displayed by default, as shown in Figure 10 on page 53.

3. Select the **File System** tab.

   The File System tab for an AT-9400 series switch with a compact flash card is shown in Figure 37 on page 127.

4. In the Default Configuration File field, enter the name of the file. When entering the file name, not the following:

   - Be sure to include the ".cfg" extension.
   - If the file is stored on a flash card in the switch, precede the name with "cflash:".

5. Click **Apply**.

   The switch searches the file system or flash memory card for the file. If it finds the file, it displays the file name in the Default Configuration File field along with the word "Exists." The file is now the active boot configuration file for the switch.

   If the switch can not locate the file, it again displays the name of the previous boot configuration file. Repeat steps 4 and 5, being sure to enter the name correctly.

6. Do one of the following:

   - To configure the switch using the parameter settings in this boot configuration file, do **not** select Save Config. Instead, reset or power cycle the switch.
   - To overwrite the settings in the configuration file with the switch's current operating settings, select **Save Config**.

Chapter 10

File Downloads and Uploads

This chapter contains the procedure for downloading a new AT-S63 image file onto the switch. This chapter also contains procedures for uploading and downloading system files, such as a boot configuration file, from the file system in the switch. This chapter contains the following sections:

- “Downloading a File” on page 134
- “Uploading a File” on page 139

Downloading a File

This procedure explains how to download a file from a TFTP server on your network to the switch using the web browser interface. You can download any of the following files:

- AT-S63 image file
- Boot configuration file
- CA certificate

> **Note**
> The CA certificate is supported only on the version of AT-S63 management software that features SSL, PKI, and SSH security.

Guidelines

Here are general guidelines to follow when performing this procedure:

- You must use TFTP to download a file from a web browser management session.
- There must be a node on your network with the TFTP server software.
- The file to download must be stored on the TFTP server node.
- You should start the TFTP server before you begin the download procedure.
- The switch receiving the downloaded file must have an IP address and subnet mask, such as a master switch of an enhanced stack. If the switch does not have an IP address, such a slave switch, you can download the file from a local management session using Xmodem or, alternatively, switch to switch. For instructions, refer to the *AT-S63 Management Software Menus Interface User's Guide*.
- You cannot download a private encryption key onto a switch, but you can a public key. However, since the switch can only use those encryption keys that it has generated itself, Allied Telesyn recommends against downloading any keys onto the switch.
- You cannot download a file to a compact flash memory card in a switch using the web browser interface.

If you are downloading the AT-S63 image file, note these additional guidelines:

- All models of the AT-9400 Series switch use the same AT-S63 image file.
- The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.

- Installing a new AT-S63 software image does not change the current configuration of a switch (for instance, IP address, subnet mask, and virtual LANs). If you want to return a switch to its default configuration values, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 52.
- This procedure gives you the option of downloading the image file into the switch's application block or the file system. The application block is the portion of flash memory in the switch reserved for the active AT-S63 image file and is separate from the file system. In most cases, you will probably want to download a new image file directly into the switch's application block so that the unit immediately begins to use it as its new operating software. However, there may be occasion when you might want to download the image file to the file system, with plans to copy it to the application block at a later date. It should be noted, however, that the only way to copy an image file in the file system to the application block is with the LOAD command in the command line interface.

Caution

Installing a new AT-S63 image file into the application block of flash memory will cause a switch reset. Some network traffic may be lost.

If you are downloading a boot configuration file, note these additional guidelines:

- A configuration file should only be downloaded onto the same model of switch where the file was originally created (for example, AT-9408LC/SP to AT-9408LC/SP). Allied Telesyn does not recommend downloading a configuration file onto a switch of a different model (for example, AT-9408LC/SP to AT-9424T/SP). Undesirable switch behavior may result.
- The configuration file is downloaded onto the switch without any modifications. If the file contains a command for assigning the switch a specific IP address, it should not be downloaded onto more than one switch. Otherwise, the same IP address will be assigned to more than one switch.
- This procedure gives you the option of downloading the file as the active boot file for the switch, in which case the switch automatically designates it as its active boot file, or just into the file system. If you choose the latter, you can designate the file as the switch's active boot file manually at a later time.

Caution

Downloading a configuration file as the switch's new active boot configuration file will cause a switch reset. Some network traffic may be lost.

To download a file, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab selected by default, as shown in Figure 39.

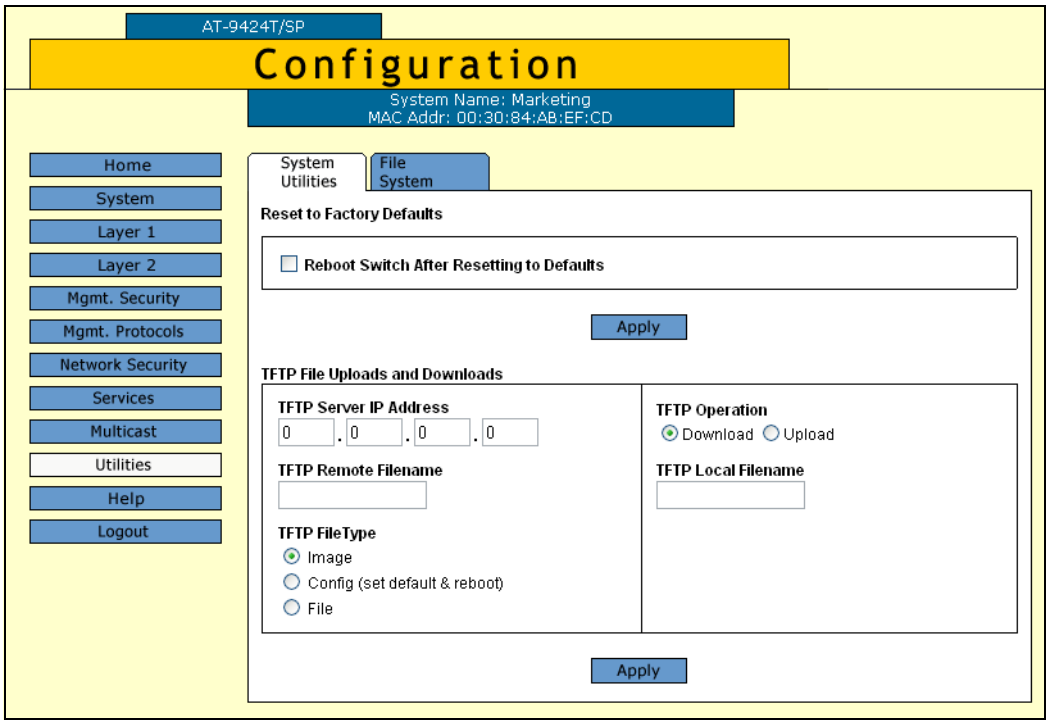

Figure 39. System Utilities Tab (Configuration)

Note

You use the top portion of the System Utilities tab to return the switch to its factory default settings. For instructions, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 52.

3. In the TFTP File Uploads and Downloads section, use the TFTP Server IP Address field to enter the IP address of the network node that contains the TFTP server software.

4. For TFTP Operation parameter, click **Download**.

5. In the TFTP Remote Filename field, enter the filename of the file on the TFTP server to be downloaded to the switch.

6. In the TFTP Local Filename field, enter a name for the file. This is the name that the switch uses to store the file in its file system. If you are downloading the AT-S63 image file into the switch's application block, enter "APPBLOCK" as the filename.

7. For the TFTP File Type, select one of the following:

   Image
   Select this option when downloading a new AT-S63 image file. This option loads the image file directly into the application block portion of flash memory so that the switch uses it as its active image file.

   Config
   Select this option when downloading a configuration file that you want the switch to use as its active boot configuration file.

   File
   Select this option to download a file to the file system. For example, you would select this option if you are downloading a CA certificate or a boot configuration file you do not want designated as the active boot configuration file.

8. Click **Apply**.

   The management software notifies you after the download is complete.

Caution
If you downloaded a new AT-S63 image file to the switch's application block, the switch decompresses it and writes it to flash memory. This can require one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file. After the file has been decompressed, the switch automatically resets. Your web browser management session ends. To continue managing the switch, you must reestablish the management session.

Note
If you downloaded a configuration file using the Config selection, the switch automatically designates it as its active configuration file and resets. At the completion of the reset, the switch operates with the parameter settings in the downloaded configuration file. The reset ends your web browser management session. To continue managing the switch, you must reestablish the management session.

Uploading a File

This procedure explains how to upload a file from the switch's file system to a TFTP server on your network using the web browser interface. You can upload any of the following files:

- Boot configuration file
- Public encryption key
- CA enrollment request
- Event log file

> **Note**
> The public key and CA enrollment request are supported only on the version of AT-S63 management software that features SSL, PKI, and SSH security.

Note the following before you begin this procedure:

- You must use TFTP to upload a file from a web browser management session.
- There must be a node on your network that contains the TFTP server software.
- You should start the TFTP server before you begin the upload procedure:
- The switch from which you are uploading a file must have an IP address and subnet mask, such as a master switch of an enhanced stack. If the switch does not have an IP address, such as a slave switch, you can upload the file from a local management session of the switch using Xmodem. For instructions, refer to the *AT-S63 Management Software Menus Interface User's Guide*.
- You cannot upload a file from a compact flash memory card using the web browser interface.

To upload a file, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab displayed by default.

Note
The top portion of the tab is used to return the switch to its factory default settings. For instructions, refer to “Returning the AT-S63 Management Software to the Factory Default Values” on page 52.

3. In the TFTP File Uploads and Downloads section, in the TFTP Server IP Address field, enter the IP address of the network node that contains the TFTP server software.
4. For the TFTP Operation parameter, click **Upload**.
5. In the TFTP Remote Filename field, enter a name for the file. This is the name that the file is stored as on the TFTP server.
6. In the TFTP Local Filename field, enter the name of the file in the switch’s file system that you want to upload to the TFTP server.
7. In TFTP File Type, select **File**.

Note
If you select Image as the TFTP File Type, the switch uploads its active AT-S63 image file to the FTP server and stores it under the name specified in step 5. There should be little or no need for you to ever upload a switch’s image file to a TFTP server.

8. Click **Apply**.

   The management software notifies you when the upload is complete.

Chapter 11

Event Logs and Syslog Servers

This chapter describes how to view or save the contents of the event logs and how to create a log output to send events to a syslog server. The event logs allow you to view information about switch activity. Sections in the chapter include:

- ❒ “Working with the Event Logs” on page 142
- ❒ “Working with Log Outputs” on page 152

For more information about the event logs and log outputs, refer to Chapter 13, “Event Logs and Syslog Servers,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Note
The event logs, even when disabled, log all AT-S63 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S63 initialization are entered into the logs only if you enable the event log feature. The default setting for the event logs is disabled.

Working with the Event Logs

The event logs contain event messages that are generated by a switch. These events can provide vital information about network activity on an AT-9400 Series switch that can help you identify and solve network problems. The information includes the time and date when an event occurred, the event's severity, the AT-S63 module that generated the event, and an event description.

The AT-9400 Series switch has two event logs. Both logs store the same event messages. There is a temporary log with a storage capacity of 4,000 events. Events in this log are lost whenever the switch is reset or power cycled. The other log is in permanent memory and has a capacity of 2,000 entries. Events in this log are retained whenever the switch is reset or power cycled.

The following procedures explain how to view the events in the event log as well as how to enable or disable the log. The procedures include:

This section includes the following topics:

- ❒ "Enabling or Disabling the Event Logs" on page 142
- ❒ "Displaying Events" on page 144
- ❒ "Clearing an Event Log" on page 150
- ❒ "Saving an Event Log to a File" on page 150

Enabling or Disabling the Event Logs

This procedure explains how to enable or disable the event logs on the switch. If you disable the logs, the AT-S63 management software will not store events in its logs and will not send events to any syslog servers you might have defined. The default setting for the event logs is enabled.

> **Note**
> Allied Telesyn recommends setting the switch's date and time if you enable the event logs. Otherwise, the entries entered in the logs and sent to a syslog server will not have the correct date and time. For instructions, refer to "Setting the System Date and Time" on page 47.

To enable or disable the event logs, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40.

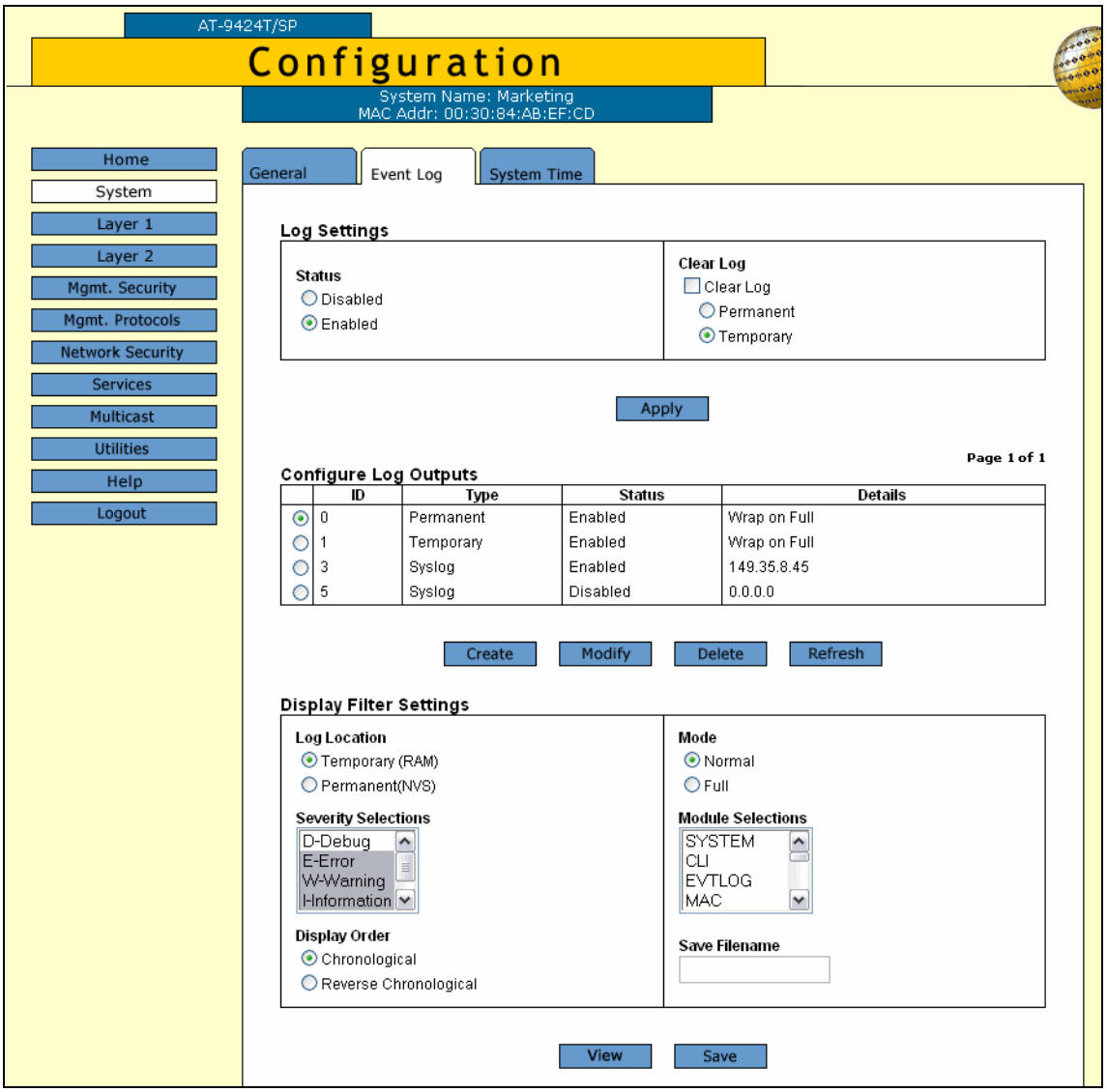

Figure 40. Event Log Tab (Configuration)

3. In the Log Settings section, for the Status, click **Enabled** to enable the event logs, or **Disabled** to disable the event logs.

   The event log feature is enabled by default.

4. Click **Apply** to activate the settings on the switch.

   If you enabled the logs, the switch immediately begins to add events to the logs and send events to defined syslog servers.

5. Select the **General** tab.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying Events

Each time that you want to view the event log, you must choose how and what you want displayed. The settings for viewing an event log are not saved.

To specify the type of events in an event log you want to display, perform the following procedure:

1. From the home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

   Note
   You can also display events by selecting Configuration from the home page and then the Event Log tab. The tab contains the same Filter Settings and Actions section as described in this procedure:

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 41.

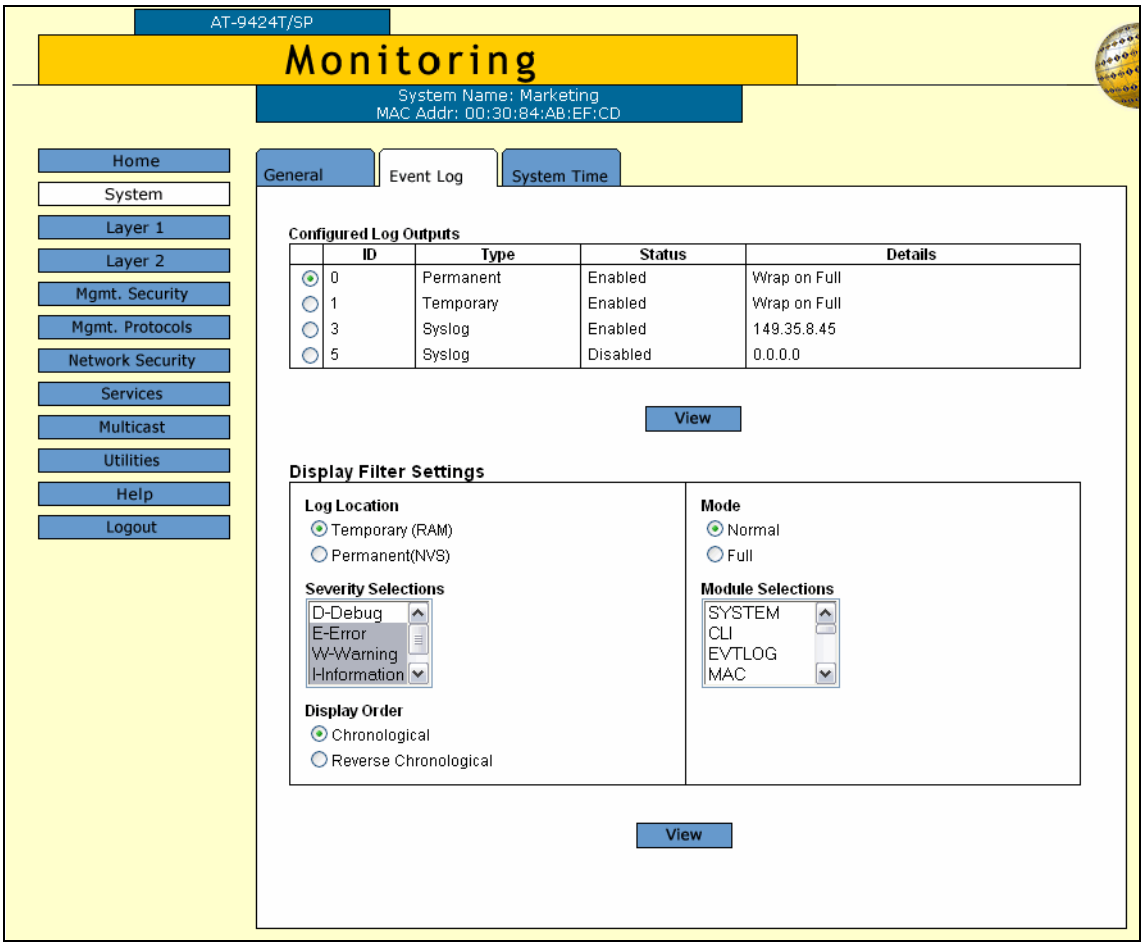

Figure 41. Event Log Tab (Monitoring)

3. In the Display Filter Settings section, for **Log Location**, click one of the following:

   Temporary (Memory)
   Displays the events stored in temporary memory. This selection stores approximately 4,000 events. If the switch has been running for some time without a reset or power cycle, select Temporary. This is the default.

   Permanent (NVS)
   Displays events stored in nonvolatile memory, which stores no more than 2,000 events. If the switch was recently reset or power cycled and you want to view the events that occurred prior to the reset, select Permanent.

4. To display events of a selected severity, in the **Severity Selections** list, select one or more of the following severity types:

   D - Debug
   Debug messages provide detailed high-volume information that is intended only for technical support personnel.

   E - Error
   Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.

   W - Warning
   Only warning messages are displayed. These messages indicate that an issue may require manager attention.

   I - Information
   Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.

   ALL
   All messages of any type are displayed.

   To select more than one severity, use <Ctrl> click.

5. To choose the chronological order of events in the display, for **Display Order**, click one of the following:

   Chronological
   Displays the events in the order from the oldest event to the most recent event. This is the default.

   Reverse Chronological
   Displays the events in from the most recent event to the oldest event.

6. To select the format of the event log, for **Mode**, click one of the following:

   Normal
   Displays the time, module, severity, and description for each event. This is the default. An example of Normal mode is shown in Figure 42 on page 148.

   Full
   Displays the same information as Normal, plus the file name, line number, and event ID. An example of Full mode is shown in Figure 43 on page 149.

7. To display events of a particular AT-S63 software module, from the **Module Selections** list, select one or more of the modules listed in Table 1. To select more than one module, use <Ctrl> click.

Table 1. AT-S63 Software Modules

Name	Description
ACL	Access control lists
ALL	All modules
CFG	Configuration file
CLASSIFIER	ACL and QoS classifiers
CLI	Command line interface commands
DOS	Denial of Service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP VLAN Registration Protocol
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	IP configuration
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management ACL
MLD	MLD snooping
PACCESS	802.1X Port-based Access Control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	Port security
PTRUNK	Static port trunks
QOS	Quality of Service
RADIUS	RADIUS authentication protocol

Table 1. AT-S63 Software Modules (Continued)

Name	Description
RPS	Redundant power supply
RRP	RRP Snooping
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	TELNET
TFTP	Trivial File Transfer Protocol
TIME	System Time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

8. Click **View**.

Figure 42 shows an example of an event log in Normal mode.

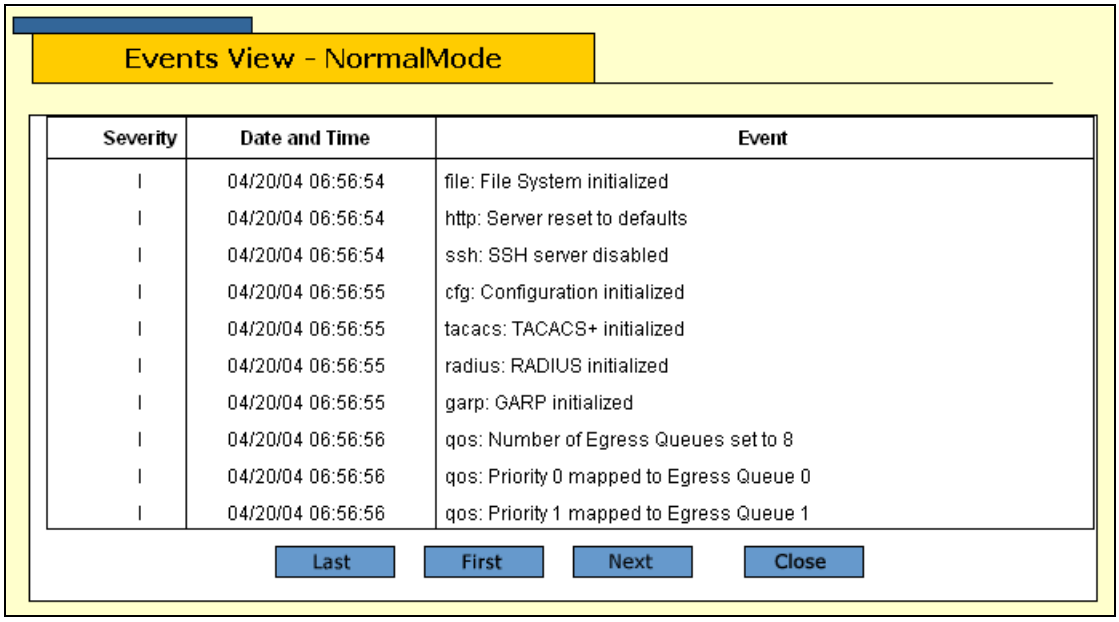
Events View - NormalMode
Severity
Date and Time
Event
I 04/20/04 06:56:54 file: File System initialized
I 04/20/04 06:56:54 http: Server reset to defaults
I 04/20/04 06:56:54 ssh: SSH server disabled
I 04/20/04 06:56:55 cfg: Configuration initialized
I 04/20/04 06:56:55 tacacs: TACACS+ initialized
I 04/20/04 06:56:55 radius: RADIUS initialized
I 04/20/04 06:56:55 garp: GARP initialized
I 04/20/04 06:56:56 qos: Number of Egress Queues set to 8
I 04/20/04 06:56:56 qos: Priority 0 mapped to Egress Queue 0
I 04/20/04 06:56:56 qos: Priority 1 mapped to Egress Queue 1
Last
First
Next
Close

Figure 42. Event Log Example Displayed in Normal Mode

The events are displayed in a table. The columns in the table shown in normal display mode are described below:

S (Severity)
The event's severity. The severity codes and their corresponding severity level and description are shown in Table 2.

Table 2. Event Severity Levels

Severity Code	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue that may require network manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

Date and Time
The date and time the event occurred.

Event
This item contains two parts. The first part is the name of the module within the AT-S63 management software that generated the event. The second part is a description of the event.

When you display the events in full mode, more information is included. Figure 43 shows the same portion of the event log in Figure 42 on page 148 but displayed in full mode.

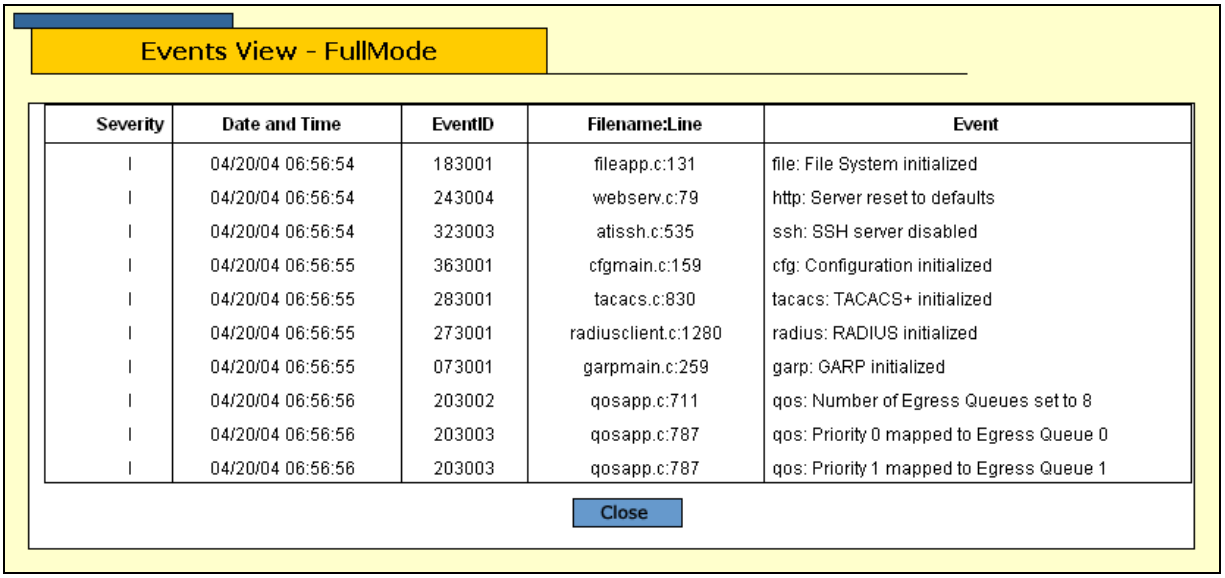
Events View - FullMode
Severity
Date and Time
EventID
Filename:Line
Event
I 04/20/04 06:56:54 183001 fileapp.c:131 file: File System initialized
I 04/20/04 06:56:54 243004 webserv.c:79 http: Server reset to defaults
I 04/20/04 06:56:54 323003 atissh.c:535 ssh: SSH server disabled
I 04/20/04 06:56:55 363001 cfgmain.c:159 cfg: Configuration initialized
I 04/20/04 06:56:55 283001 tacacs.c:830 tacacs: TACACS+ initialized
I 04/20/04 06:56:55 273001 radiusclient.c:1280 radius: RADIUS initialized
I 04/20/04 06:56:55 073001 garpmain.c:259 garp: GARP initialized
I 04/20/04 06:56:56 203002 qosapp.c:711 qos: Number of Egress Queues set to 8
I 04/20/04 06:56:56 203003 qosapp.c:787 qos: Priority 0 mapped to Egress Queue 0
I 04/20/04 06:56:56 203003 qosapp.c:787 qos: Priority 1 mapped to Egress Queue 1
Close

Figure 43. Event Log Example Displayed in Full Mode

In addition to the information displayed in Normal mode, the Full mode also displays additional columns in the table, as described below:

Event ID
A unique, random number assigned to each event.

Filename:Line
The AT-S63 software source file name and the line number in that source file that produced the event.

9. Click one of the following buttons to scroll through the event log:

   Last - Last page

   First - First page

   Next - Next page

   Previous - Previous page

   Close - Closes the log

   To clear the current event log, go to “Clearing an Event Log” on page 150.

Clearing an Event Log

You can clear an event log to remove old events and start fresh. To clear an event log, do the following:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **Event Log** tab.

   The Event log tab is shown in Figure 40 on page 143.

3. In the Log Settings section, click the **Clear Log** checkbox.

4. Click the button next to the event log you want to clear, either Permanent or Temporary.

5. Click **Apply** to activate the settings on the switch.

Saving an Event Log to a File

You can save an event log to a file to review later. The file is saved as an ASCII file in the switch’s file system, from where you can view it or upload it to your management workstation or a TFTP server.

To save an event log to a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **Event Log** tab.

   The Event log tab is shown in Figure 40 on page 143.

3. In the **Display Filter Settings** section, select the log and the type of events you want to save to the file. For instructions, refer to steps 3 to 7 in "Displaying Events" on page 144.

4. In the **Save Filename** field, enter a name for the file. The name can be up to 16 alphanumeric characters. The name must include the `.log` file name extension.

5. Click **Save**.

   The log file is saved to the switch's file system as an ASCII file.

6. To upload the file to your management station for viewing or sending with an email, refer to "Uploading a File" on page 139.

Working with Log Outputs

Instead of checking the log files on each individual switch, you can create an output definition that defines the events that are sent to a syslog server. From this central point, you can monitor all the AT-9400 Series switches in your network. This is called a log output file. For more information about log output files, refer to Chapter 13, “Event Logs and Syslog Servers,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

This section contains the following topics:

- “Configuring a Log Output Definition,” next
- “Viewing a Log Output Definition” on page 154
- “Modifying a Log Output Definition” on page 156
- “Deleting a Log Output Definition” on page 158

Configuring a Log Output Definition

To configure a log output, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **Event Log** tab.

   The Event log tab is shown in Figure 40 on page 143.

3. In the Configure Log Outputs section, click **Create**.

   The Create Log Output page is shown in Figure 44.

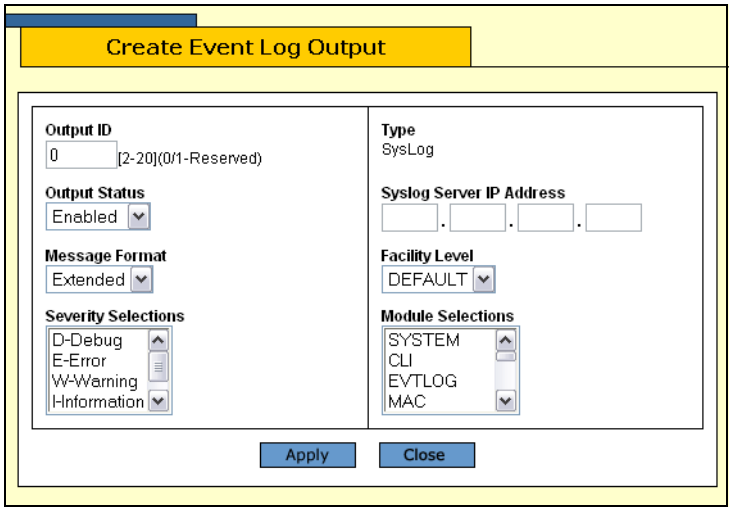

Figure 44. Create Event Log Output Page

4. Configure the following parameters as necessary:

   Output ID
   An ID number for the log output.

   Output Status
   Specifies whether or not the output is sent to the syslog server. The options are:

   Enabled - Enables the log output. Event messages are sent to the defined syslog server.

   Disabled - Disables the log output. Event messages are not sent to the defined syslog server.

   Message Format
   Specifies the format of the messages sent to the syslog server. The options are:

   Extended - Sends the time, module, severity, description, file name, line number, and event ID. This is the default.

   Normal - Sends the time, module, severity, and description for each event.

   Severity Selections
   Specifies the severity of events you want to send to the syslog server. The possible options are:

   ALL - Sends all event messages of the following types. This is the default.

   Error - Sends only error event messages. Error messages indicate that the switch operation is severely impaired.

   Warning - Sends only warning event messages. These messages indicate that an issue may require manager attention.

   Information - Sends only informational event messages. Informational messages display useful information that you can ignore during normal operation.

   Debug - Sends debug event messages. These events provide detailed high-volume information that is intended only for technical support personnel.

   Use <Ctrl>+click to select more than one severity at a time.

   Type
   The only available type is Syslog and you cannot change this.

   Syslog Server IP Address
   The IP address of the syslog server.

Facility Level
The numerical code to be added to the entries sent to the syslog server to group the entries according to the module or switch that produced them.

The facility levels are described in Table 3.

Table 3. Default Syslog Facilities

Facility	Mapped Event Log Modules and Events
Default	This facility number applies the functional groupings defined in the RFC 3164 standard.
local 1 through local 7	An identifier to assign to specific switches or groups of switches.

Note
For further information about the syslog facility levels, refer to Chapter 13, “Event Logs and Syslog Servers” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Module Selections
Specifies the AT-S63 management software module(s) whose events you want to send to the syslog server. To select more than one, use <Ctrl>+click. For a list of modules, refer to Table 1 on page 147.

5. Click **Apply**.

   The switch creates the new log output server definition and immediately begins sending events to the server if you enabled the Message Generation option.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Viewing a Log Output Definition

To view an existing log output definition, perform the following procedure:

1. From the home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 41 on page 145.

3. In the Configured Log Outputs section, select a log output from the list and click **View**.

The View Log Output page is shown in Figure 45.

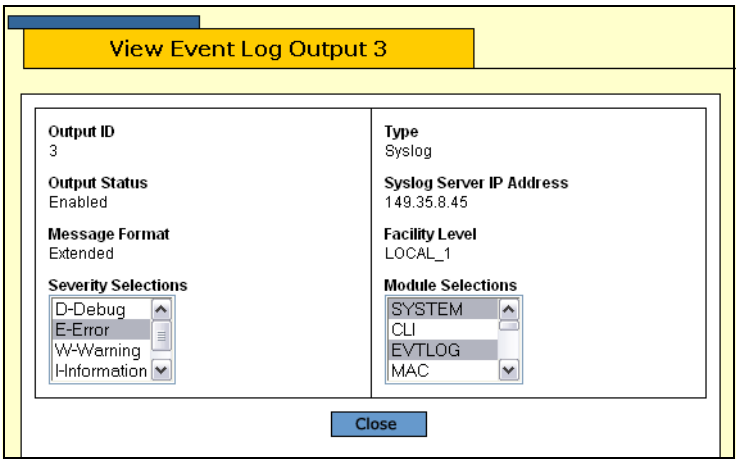

Figure 45. View Event Log Output Page

This page displays the following information:

Output ID
An ID number for the log output.

Output Status
Whether or not the output is sent to the syslog server, either enabled or disabled.

Message Format
The format of the messages sent to the syslog server.

Severity Selections
The severity of events sent to the syslog server. Scroll the list to view all the selections.

Type
The only available type is Syslog and you cannot change this.

Syslog Server IP Address
The IP address of the syslog server.

Facility Level
The numerical code to be added to the entries sent to the syslog server to group the entries according to the module or switch that produced them.

Module Selections
Specifies the AT-S63 management software module(s) whose events you want to send to the syslog server. Scroll the list to view all the modules that have been selected for this log output.

4. When you are done, click **Close**.

Modifying a Log Output Definition

To modify a log output definition, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **Event Log** tab.

   The Event log tab is shown in Figure 40 on page 143.

3. In the Configure Log Outputs section, Select the log output file that you want to modify and click **Modify**.

   The Configure Log Outputs section is shown in Figure 46.

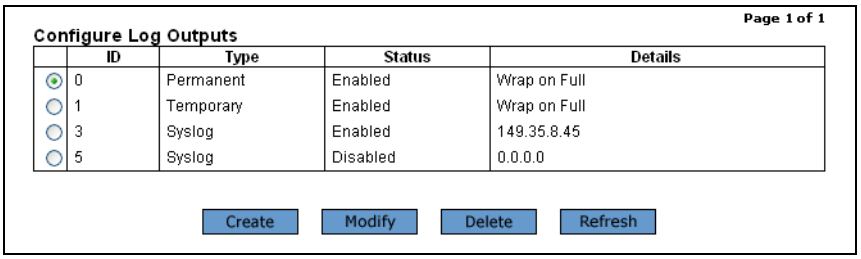

Figure 46. Configure Log Outputs Section

The Modify Event Log Output page is shown in Figure 47.

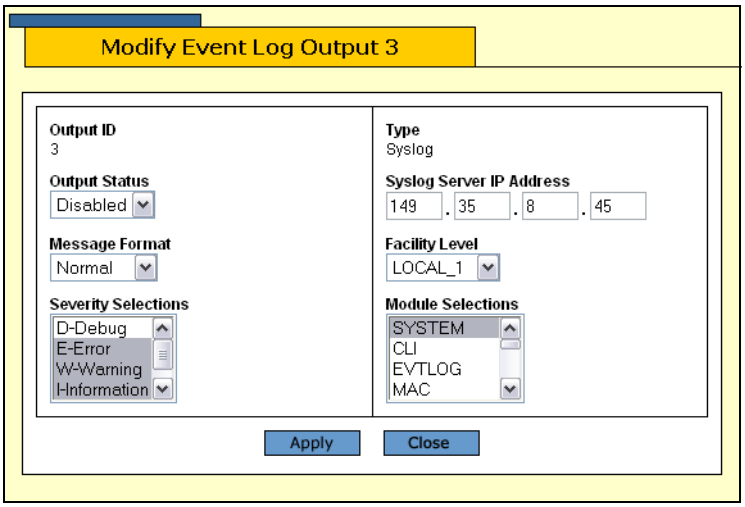

Figure 47. Modify Event Log Output Page

4. Modify the following parameters as necessary:

   Output ID
   An ID number for the log output.

Output Status
Specifies whether or not the output is sent to the syslog server. The options are:

Enabled - Sends the output to the syslog server.

Disabled - The output is not sent to the syslog server even if an IP address is defined.

Message Format
Specifies the format of the messages sent to the syslog server. The options are:

Extended - Displays the time, module, severity, description, file name, line number, and event ID. This is the default.

Normal - Displays the time, module, severity, and description for each event.

Severity Selections
Specifies the severity of events you want to send to the syslog server. The possible options are:

ALL - All messages of the following types are displayed. This is the default.

Error - Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.

Warning - Only warning messages are displayed. These messages indicate that an issue may require manager attention.

Information - Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.

Debug - Debug messages provide detailed high-volume information that is intended only for technical support personnel.

Use <Ctrl>+click to select more than one severity at a time.

Type
The only available type is Syslog and you cannot change this.

Syslog Server IP Address
The IP address of the syslog server.

Facility Level
The numerical code to be added to the entries sent to the syslog server to group the entries according to the module or switch that produced them.

The facility levels are described in Table 3 on page 154.

Module Selections
Specifies the AT-S63 management software module(s) whose events you want to send to the syslog server. To select more than one, use <Ctrl>+click. For a list of modules, refer to Table 1 on page 147.

5. Click **Apply** to apply the changes or **Close** to close the page without making changes.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Log Output Definition

To delete a log output, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **Event Log** tab.

   The Event log tab is shown in Figure 40 on page 143.

3. In the Configure Log Outputs section, Select the log output file that you want to modify and click **Delete**.

   The log output definition is deleted from the list.

Chapter 12
Classifiers

A classifier defines a traffic flow. You use classifiers with access control lists to filter ingress traffic on a port and with Quality of Service policies to regulate different traffic flows that pass through a switch.

This chapter contains the following sections:

- ❒ “Configuring a Classifier” on page 160
- ❒ “Modifying a Classifier” on page 166
- ❒ “Deleting a Classifier” on page 168
- ❒ “Displaying the Classifiers” on page 169

Note
For background information about classifiers, refer to Chapter 14, “Classifiers,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring a Classifier

This procedure explains how to create an ACL. It is a good idea before performing this procedure to jot down on paper the ID number(s) of the classifier(s) you want to assign to the ACL and the action of the ACL, which is either Permit or Deny. An action of Permit instructs the port to accept packets from the defined traffic flow of the classifier, while an action of Deny discards the packets. Having this information handy will make it easier for you to perform the procedure. To view the classifier ID numbers and specifications, refer to “Displaying the Access Control Lists” on page 178.

To configure a classifier, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

   Note
   You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Network Security menu option.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **Classifier** tab.

The Classifier tab is shown in Figure 48.

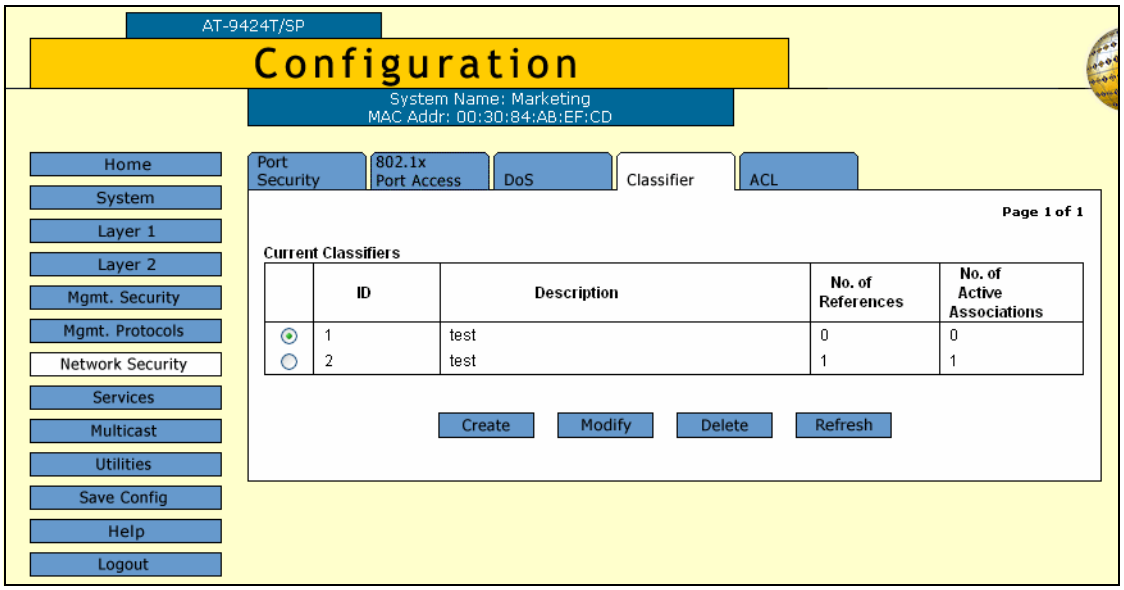

Figure 48. Classifier Tab (Configuration)

The tab lists the current classifiers on the switch. The columns are defined here:

ID
The ID number of the classifier.

Description
A description of the classifier.

No. of References
The number of active and inactive ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS is assigned to at least one switch port, while an inactive ACL or QoS policy is currently not assigned to any port. If this column is 0 (zero), the classifier is not assigned to any ACLs or policies, active or inactive.

No. of Active Associations
The number of active ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one switch.

4. Click **Create**.

The Create Classifier page is shown in Figure 49.

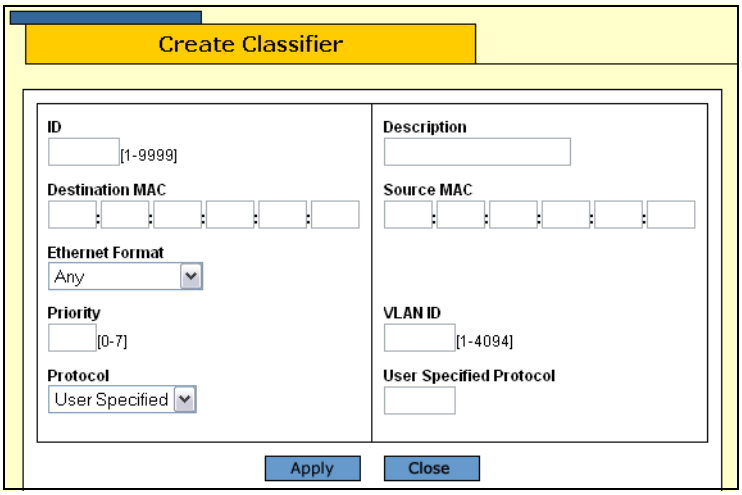

Figure 49. Create Classifier Page

Some of the variables and settings display additional selections. For example, selecting IP as the Protocol displays the selections shown in Figure 50.

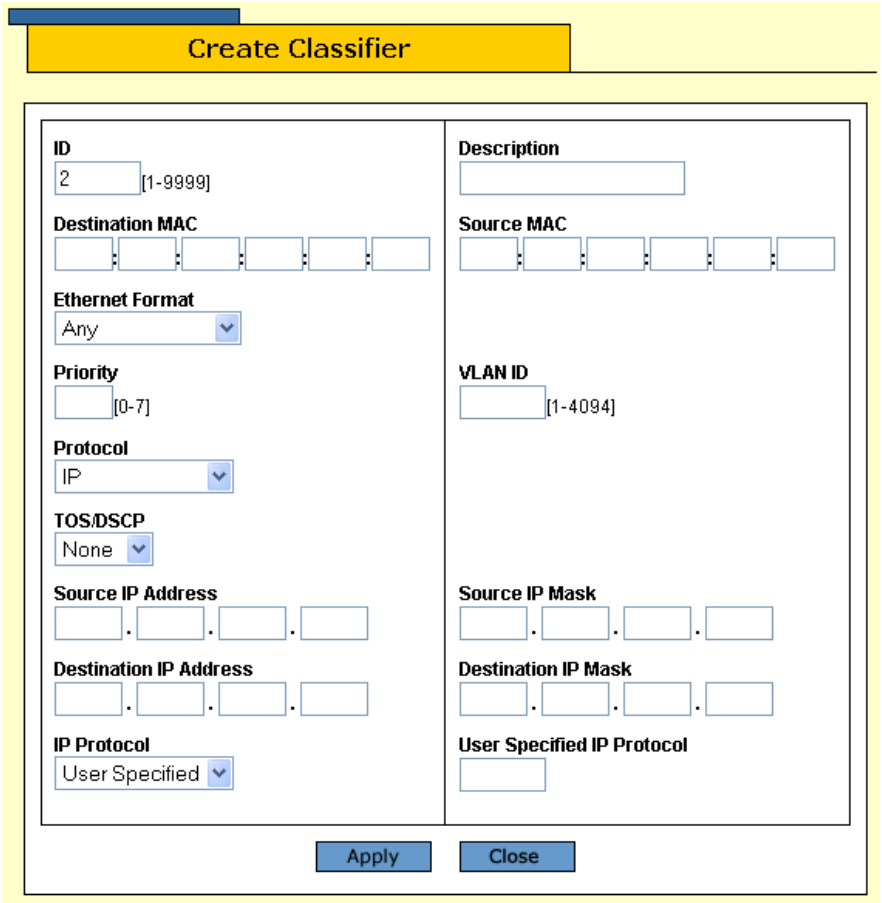

Figure 50. Create Classifier Page - IP Protocol

5. Configure the following parameters as desired:

   ID
   Specifies an ID number for the classifier. Every classifier on the switch must have a unique ID number. The range is 1 to 9999. This parameter is required.

   Description
   Specifies a description for the classifier. A description can be up to fifteen alphanumeric characters. Spaces are allowed.

   Destination MAC
   Defines a traffic flow by its destination MAC address.

   Source MAC
   Defines a traffic flow by its source MAC address.

   Ethernet Format
   Defines a traffic flow by the format of the Ethernet packets. Selections are:

   - Untagged - Ethernet II untagged packets
   - Tagged - Ethernet II tagged packets
   - 802.2 untagged - Ethernet 802.2 untagged packets
   - 802.2 tagged - Ethernet 802.2 tagged packets

   Priority
   Defines a traffic flow by the user priority level in tagged Ethernet frames. The range is 0 to 7.

   VLAN ID
   Defines a traffic flow of tagged packets by its VLAN ID number. The range is 1 to 4094.

   Protocol
   Defines a traffic flow as one of the following Layer 2 protocols:

   - User Specified
   - IP
   - ARP
   - RARP

   User Specified Protocol
   Defines a traffic flow of a Layer 2 protocol by its protocol number. The number can be entered in either decimal or hexadecimal format. For the latter, precede the number with "0x". To use this parameter, the Protocol parameter must be set to User Specified.

TOS/DSCP
Defines a traffic flow by its Type of Service or DSCP value. To set this parameter, the Protocol parameter must be set to IP. Options are:

- TOS (Type of Service)
- DSCP

TOS
Defines a traffic flow by its Type of Service value. The range is 0 to 7. To set this value, the TOS/DSCP parameter must be set to TOS.

DSCP
Defines a traffic flow by its DSCP value. The range is 0 to 63. To set this value, the TOS/DSCP parameter must be set to DSCP.

IP Protocol
Defines a traffic flow of a Layer 3 protocol. To set this parameter, the Protocol variable must be set to IP. Options are:

- User Specified
- TCP
- UDP
- ICMP
- IGMP

User Specified IP Protocol
Defines a traffic flow of a Layer 3 protocol by its protocol number. The number can be entered in either decimal or hexadecimal format. If you use the latter, precede the number with “0x”. To set this parameter, the IP Protocol parameter must be set to User Specified.

Source IP Address
Source IP Mask
Defines a traffic flow by a source IP address. The address can be of a specific node or a subnet.

You do not need to include a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the Class C subnet address 149.11.11.0 would have the mask “255.255.255.0”.

Destination IP Address
Destination IP Mask
Defines a traffic flow by its destination IP address. The address can be of a specific node or a subnet.

You do not need to include a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on

the corresponding bit of the IP address, while a "0" indicates that it should not. For example, the Class C subnet address 149.11.11.0 would have the mask "255.255.255.0".

TCP Source Port
Defines a traffic flow by source TCP port. To set this parameter, IP Protocol must be set to TCP.

TCP Destination Port
Defines a traffic flow by destination TCP port. To set this parameter, IP Protocol must be set to TCP.

TCP Flags
Defines a traffic flow by TCP flag. To set this parameter, IP Protocol must be set to TCP. Options are

- URG - Urgent
- ACK - Acknowledgement
- RST - Reset
- PSH - Push
- SYN - Synchronization
- FIN - Finish

UDP Source Port
Defines a traffic flow by source UDP port. To set this parameter, IP Protocol must be set to UDP.

UDP Destination Port
Defines a traffic flow by a destination UDP port. To set this parameter, IP Protocol must be set to UDP.

User Specified Protocol
Defines a traffic flow by a protocol other than one of those listed in the Protocol or IP Protocol list. To set this parameter, Protocol must be set to User Specified. Alternatively, you can set this parameter if IP Protocol is set to User Specified.

6. Click **Apply**.

   The new classifier is created on the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Classifier

This procedure explains how to modify a classifier. If the classifier you want to modify is currently assigned to an active ACL or QoS policy, you must first remove the port assignments from the ACL or policy before you can modify the classifier. Once you have finished modifying the classifier, you can reassign the ports again to the ACL or QoS policy.

To modify a classifier, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

   Note
   You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Network Security menu option.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 48 on page 161.

4. Click **Modify**.

   The Modify Classifier page is shown in Figure 51.

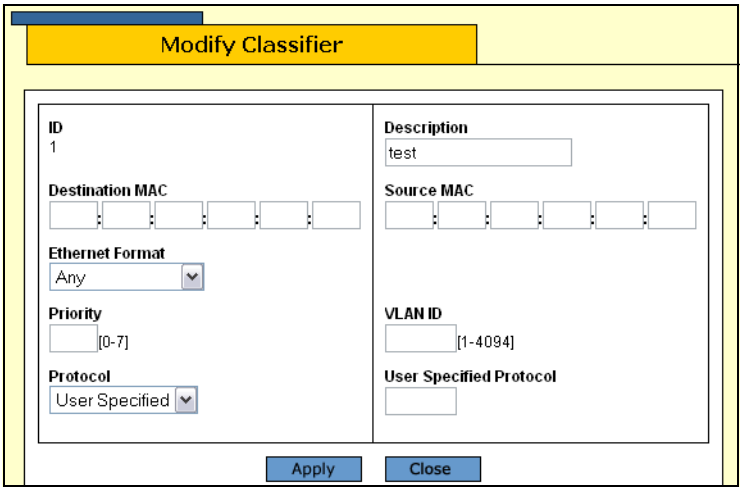

Figure 51. Modify Classifier Page

5. Modify the parameters as necessary: For descriptions of the parameters, refer to "Configuring a Classifier" on page 160.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Classifier

To delete a classifier, perform the following procedure:

Note
You cannot delete a classifier if it belongs to an ACL or QoS policy. You must first remove it from the ACL or policy before you can delete it.

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

   Note
   You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Network Security menu option.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 48 on page 161.

4. Click the button next to the classifier you want to delete and click **Delete**.

   The classifier is deleted from the switch.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Classifiers

To display the classifiers, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

   Note
   You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Services menu option.

2. From the Monitoring menu, select **Services**.

   The Services menu is displayed with the CoS tab selected by default, as shown in Figure 62 on page 188.

3. Select the **Classifiers** tab.

   The Classifiers tab is shown in Figure 52.

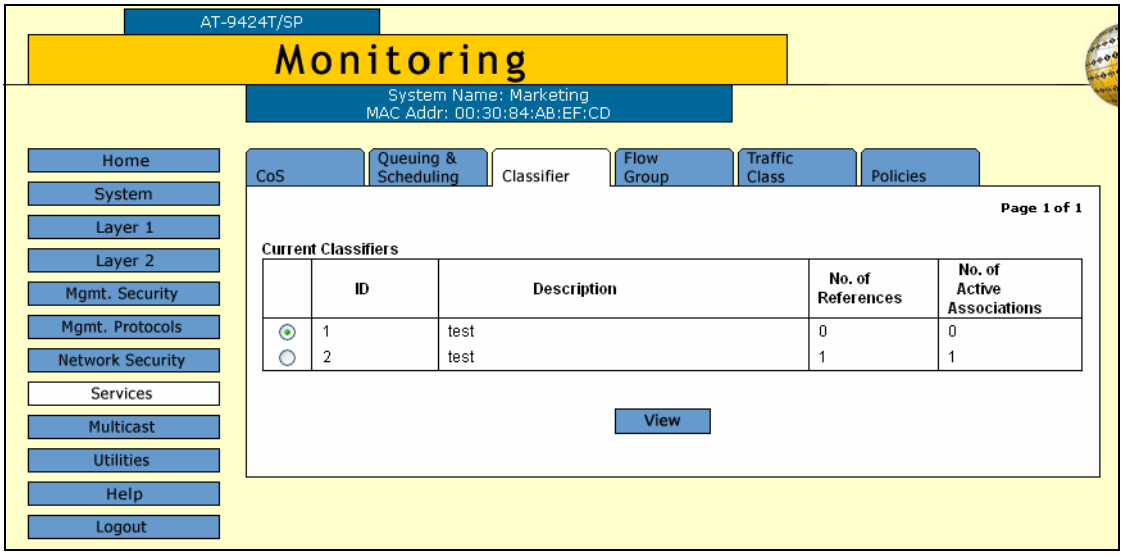

Figure 52. Classifier Tab (Monitoring)

The Classifier tab displays a table of the currently configured classifiers that contains the following columns of information:

ID
The ID number of the classifier.

Description
A description of the classifier.

No. of References
The number of active and inactive ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS is assigned to at least one switch port, while an inactive ACL or QoS policy is currently not assigned to any port. If this column is 0 (zero), the classifier is not assigned to any ACLs or policies, active or inactive.

No. of Active Associations
The number of active ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one switch.

4. To display detailed information about a classifier, select the classifier and click **View**.

   An example of the View Classifier page is shown in Figure 53.

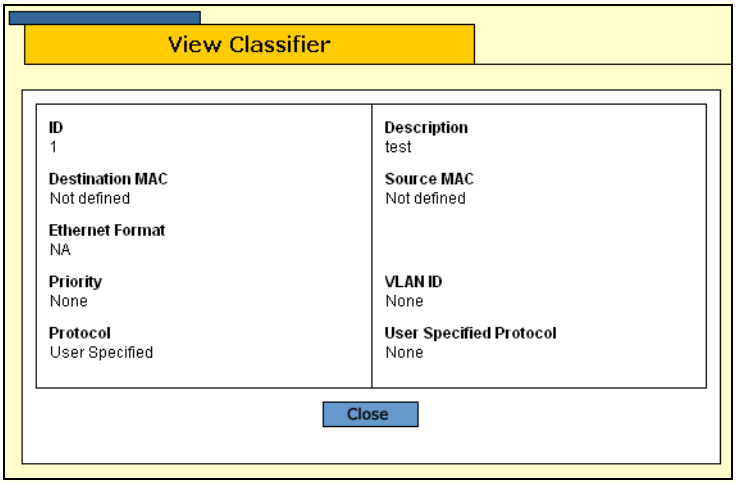

Figure 53. View Classifier Page

   For descriptions of the variables, refer to “Configuring a Classifier” on page 160.

5. Click **Close** to close the page.

Chapter 13

Access Control Lists

An access control list (ACL) is a tool for managing network traffic. This chapter contains the following sections:

- ❒ “Configuring an Access Control List” on page 172
- ❒ “Modifying an Access Control List” on page 175
- ❒ “Deleting an Access Control List” on page 177
- ❒ “Displaying the Access Control Lists” on page 178

Note
For background information about access control lists, refer to Chapter 15, “Access Control Lists,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring an Access Control List

This procedure explains how to create an ACL. Before starting this procedure, jot down on paper the ID number(s) of the classifier(s) you want to assign to the ACL and the action of the ACL, which is either Permit or Deny. An action of Permit instructs the port to accept packets from the defined traffic flow of the classifier, while an action of Deny discards the packets. Having this information handy will make it easier for you to perform the procedure. To view the classifier ID numbers and specifications, refer to “Displaying the Classifiers” on page 169.

To configure an access control list, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **ACL** tab.

   The ACL tab is shown in Figure 54.

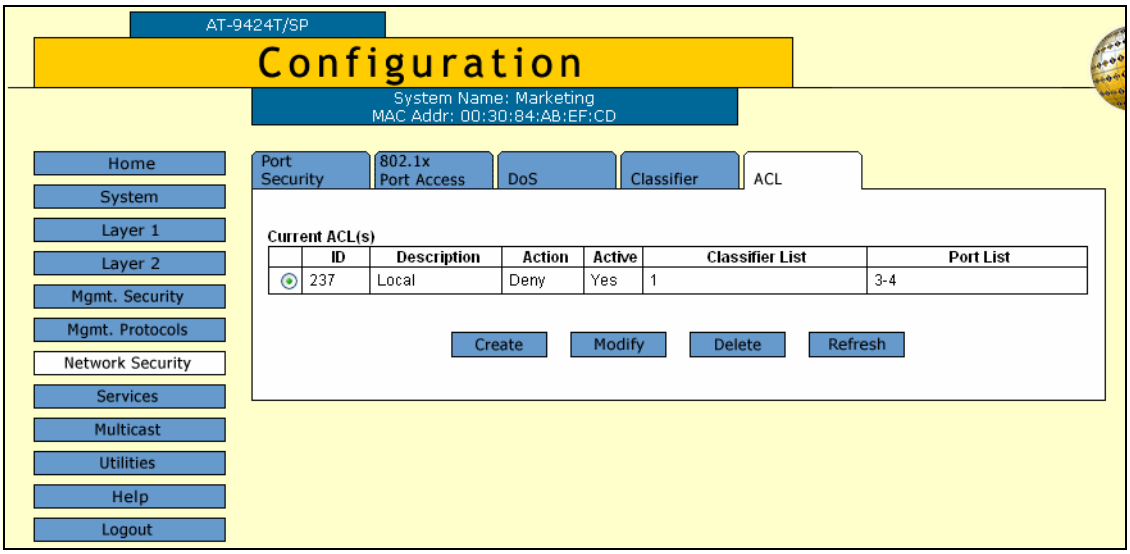

Figure 54. ACL Tab (Configuration)

4. Click **Create**.

   The Create ACLs page is displayed, as shown in Figure 55.

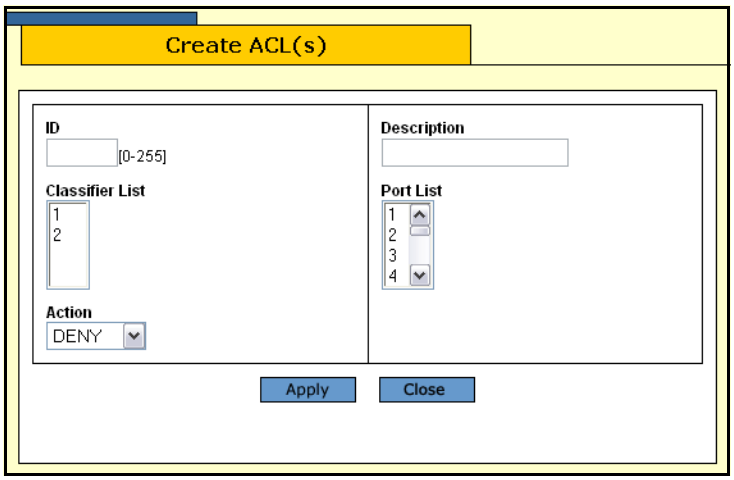

Figure 55. Create ACLs Page

5. Configure the following parameters:

   ID
   Use this field to enter an ID number for the ACL. Every ACL on the switch must have a unique ID number. The range is 0 to 255.

   Classifier List
   Use this list to select the classifier you want to assign to this ACL. You can assign more than one classifier to an ACL. To select multiple classifiers, hold down the Ctrl key while making your selections. To view the classifiers on a switch, refer to "Displaying the Classifiers" on page 169. An ACL must have at least one classifier.

   Action
   Use this menu to specify the action of the ACL. Deny, which is the default, discards ingress packets that match the defined traffic flow of the classifier. Permit accepts the packets. The default is Deny.

   Description
   Use this field to enter a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces. A description is optional.

   Port List
   Use this list to specify the port where you want to assign the ACL. You can assign an ACL to more than one port. To select multiple ports, hold down the Ctrl key while making your selections. You do not have to assign an ACL to a port when you initially create it. However, an ACL that is not assigned to any port is considered inactive.

6. Click **Apply**.

   The new ACL is immediately activated on the specified ports. If you did not specify any ports for the ACL, the ACL is created but remains inactive until you assign it to a port.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an Access Control List

To modify an access control list, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **ACL** tab.

   The ACL tab is shown in Figure 54 on page 172.

4. Select the ACL you want to modify and click **Modify.**

   The Modify ACLs page is displayed, as shown in Figure 56.

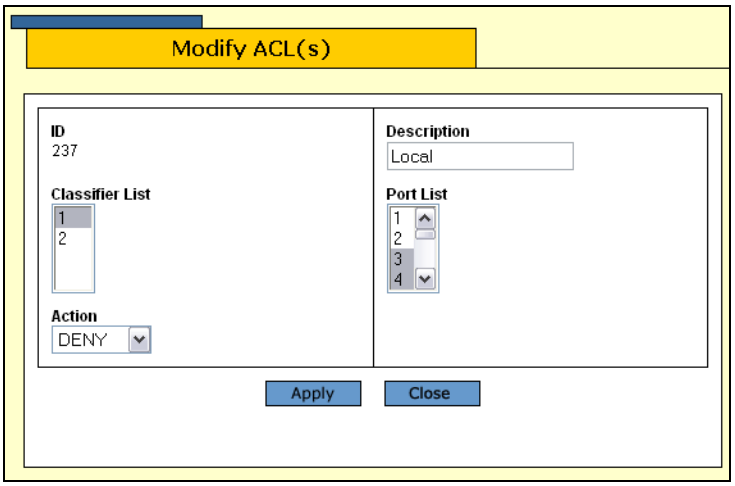

Figure 56. Modify ACLs Page

5. Configure the following parameters as necessary:

   ID
   The ID number of the ACL. You cannot change this value.

   Classifier List
   Use this list to select the classifier you want to assign to this ACL. You can assign more than one classifier to an ACL. To select multiple classifiers, hold down the Ctrl key while making your selections. To view the classifiers, refer to "Displaying the Classifiers" on page 169. An ACL must have at least one classifier.

Action
Use this menu to specify the action of the ACL. Deny, which is the default, discards ingress packets that match the defined traffic flow of the classifier. Permit accepts the packets. The default is Deny.

Description
Use this field to enter a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces. Entering a description is optional.

Port List
Use this list to specify the port where you want to assign the ACL. You can assign an ACL to more than one port. To select multiple ports, hold down the Ctrl key while making your selections. To remove the ACL from its current port assignments without assigning it to any new ports, hold down the Ctrl key while deselecting the currently assigned ports. An ACL that is not assigned to any port is considered inactive.

6. Click **Apply.**

   Changes to the ACL are immediately implemented on the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an Access Control List

To delete an access control list, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **ACL** tab.

   The ACL tab is shown in Figure 54 on page 172.

4. Select the ACL you want to delete and click **Delete**. You can delete only one access control list at a time.

   The ACL is immediately deleted from the switch.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Access Control Lists

To display the current ACLs, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Network Security**.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 160 on page 395.

3. Select the **ACL** tab.

   The ACL tab is shown in Figure 57.

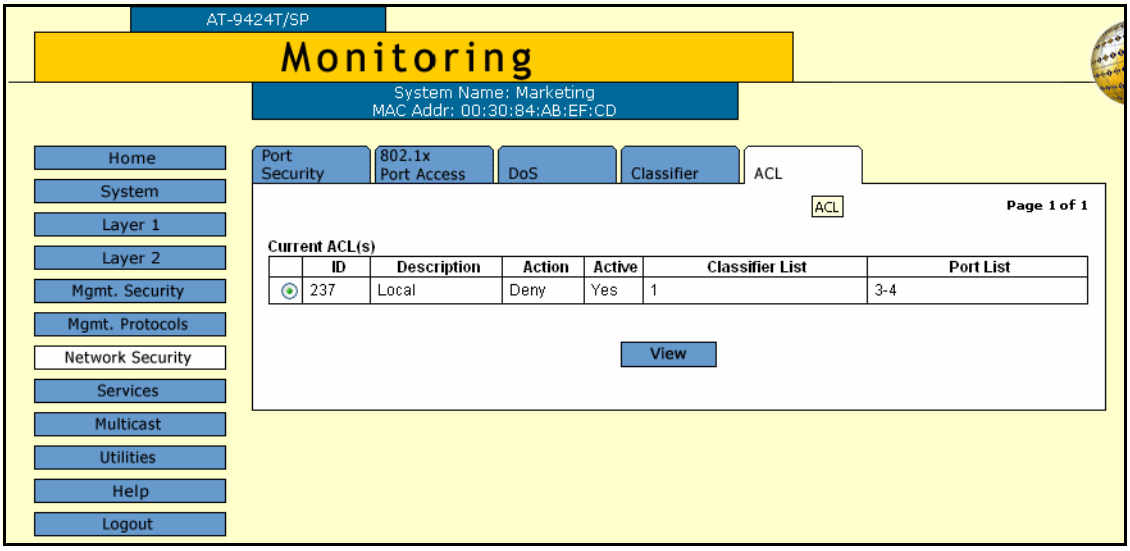

Figure 57. ACL Tab (Monitoring)

The ACL tab displays a table of the currently configured ACLs that contains the following columns of information:

ID
The ID number for the ACL.

Description
A description of the ACL.

Action
The ACL action of Permit or Deny. An action of Permit means the port accepts the packets that meet the criteria of the classifiers assigned to the ACL. An action of Deny means the port discards the packets, unless the packets also match the criteria of a Permit ACL, in which

case the packets are accepted by the port, because a Permit ACL overrides a Deny ACL.

Active
Whether or not the ACL is active. A status of Yes means that the ACL is assigned to at least one port on the switch. A status of No means the ACL is not assigned to any ports and therefore is inactive.

Classifier List
The classifiers assigned to the ACL.

Port List
The port assignments of the ACL.

4. To view the same information for each ACL, select the ACL and click **View.**

   The View ACLs page opens, as shown in Figure 58.

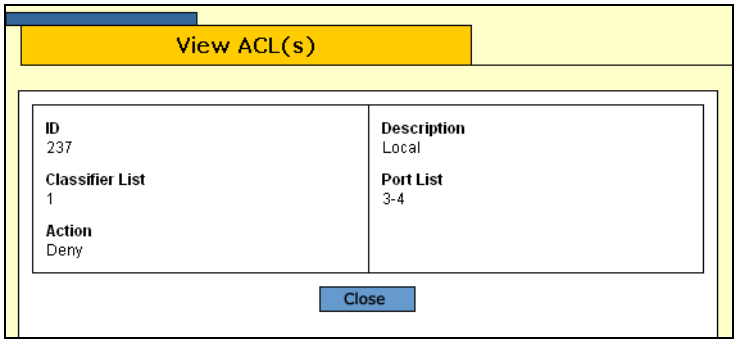

Figure 58. View ACLs Page

   The View ACLs page displays the following information:

   ID
   The ID number for the ACL.

   Description
   The description of the ACL.

   Classifier List
   The classifiers assigned to this ACL.

   Port List
   The ports where the ACL is assigned.

   Action
   The ACL action of Permit or Deny. An action of Permit means the port accepts the packets that meet the criteria of the classifiers assigned to the ACL. An action of Deny means the port discards the packets, unless the packets also match the criteria of a Permit ACL.

5. Click **Close**.

Chapter 14

Class of Service

This chapter contains instructions on how to configure Class of Service (CoS). This chapter contains the following procedures:

- ❒ “Configuring CoS” on page 182
- ❒ “Mapping CoS Priorities to Egress Queues” on page 184
- ❒ “Configuring Egress Scheduling” on page 186
- ❒ “Displaying the CoS Settings” on page 188
- ❒ “Displaying the QoS Schedule” on page 190

Note
For background information on CoS, refer to Chapter 16, “Class of Service,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring CoS

This procedure sets the Class of Service priority level for ingress untagged packets on a port. The priority level dictates which priority queue the packets are stored in on the egress port. In the default settings, ingress untagged packets on a port are assigned a priority level of 0 and are stored in egress queue Q1 on the egress port. This procedure also overrides the priority level in tagged ingress packets. To adjust the mappings of priority levels to egress queues, refer to “Mapping CoS Priorities to Egress Queues” on page 184.

To change the CoS priority level on a port, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59.

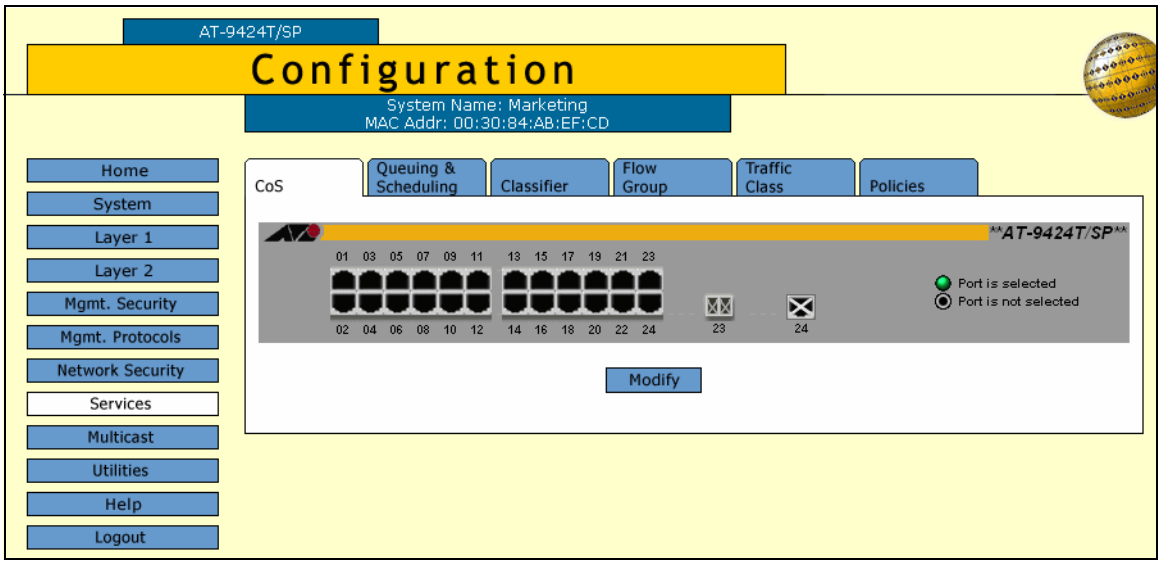

Figure 59. CoS Tab (Configuration)

3. Select the ports whose CoS settings you want to configure and click **Modify**.

The CoS Setting for Port page is shown in Figure 60.

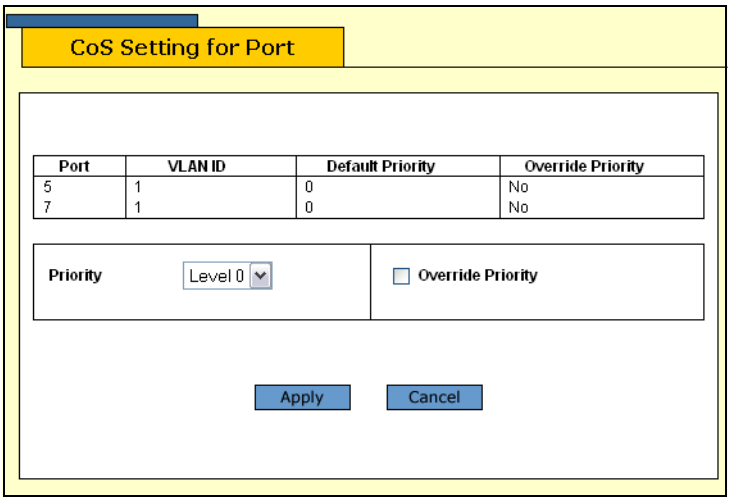

Figure 60. CoS Setting for Port Page

4. Use the Priority list to select a new Class of Service priority level for the port. The default is level 0. The new priority level will apply to all ingress untagged packets. (If you perform Step 5 and override the priority level in tagged packets, the new priority level will also apply to all ingress tagged packets.)

5. If you are configuring a tagged port and you want the port to ignore the priority tag in the packets, click the **Override Priority** option. A check in the box indicates this feature is activated. All tagged packets are directed to the egress queue specified in Step 4.

   Note
   The switch does not change the tagged information in a tagged packet. A tagged packet exits the switch with the same priority level that it had when it entered.

   The default for this parameter is No, meaning that the priority level of a tagged packet is determined by the tagged information in the packet itself.

6. Click **Apply**.

   Configuration changes are immediately activated on the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues. To change the mappings, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Queuing & Scheduling** tab.

   The Queuing & Scheduling tab is shown in Figure 61.

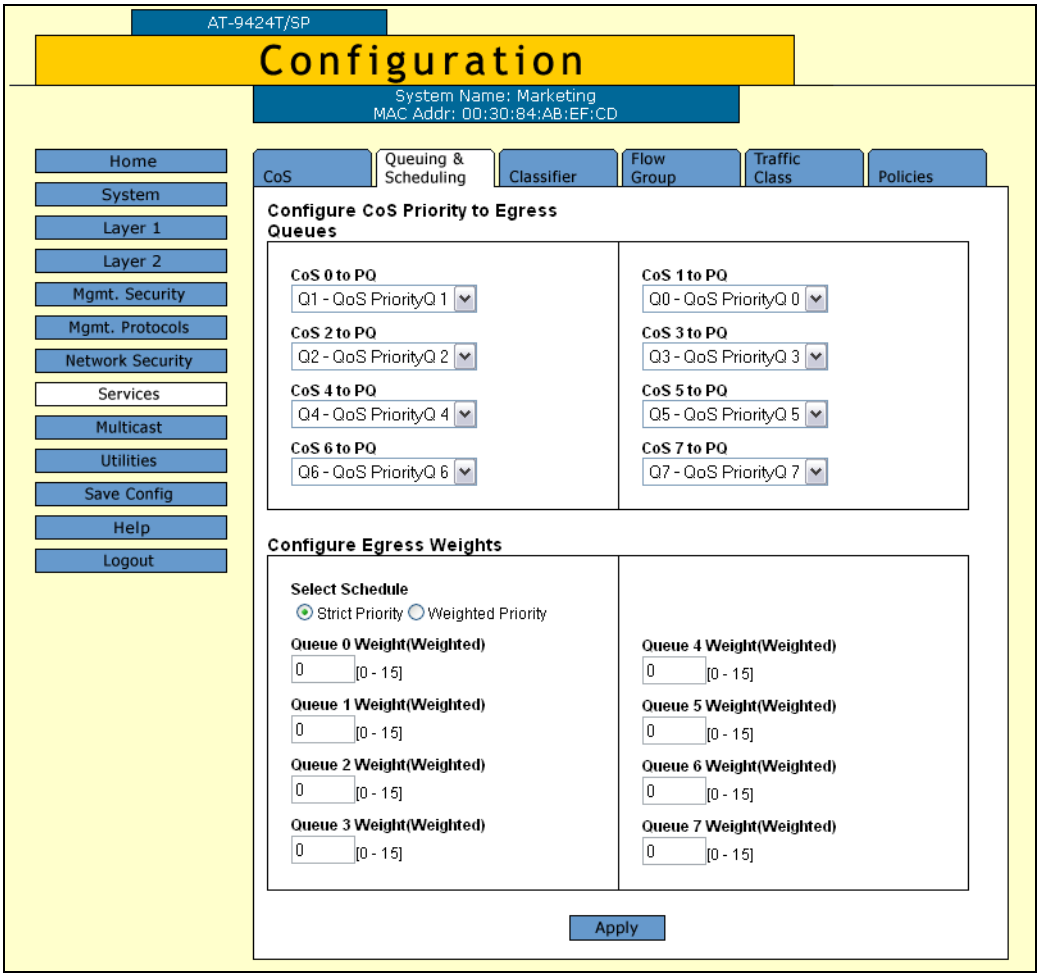

Figure 61. Queuing & Scheduling Tab (Configuration)

Note
The Configure Egress Weights section in the tab is explained in the next procedure, "Configuring Egress Scheduling" on page 186.

The default values are listed in Table 4.

Table 4. Default Mappings of IEEE 802.1p Priority Levels to Egress Priority Queues

IEEE 802.1p Priority Level	Egress Port Priority Queue
0	Q1
1	Q0
2	Q2
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7

4. In the Configure CoS Queues to Egress Queues section of the tab, click the list for a CoS priority whose queue assignment you want to change and select the new queue.

   For example, to direct all ingress tagged packets with a CoS priority of 5 to egress queue Q3, you would use the list in **CoS 5 to PQ** and select **Q3 - QoS PriorityQ 3.**

5. If desired, repeat Step 4 to change the egress queue assignment of other CoS priorities.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring Egress Scheduling

This procedure explains how to select and configure a scheduling method for Class of Service. Scheduling determines the order in which the ports handle packets in their egress queues. For an explanation of the two scheduling methods, refer to Chapter 16, “Class of Service,” in the *AT-S63 Management Software Menus Interface User’s Guide*. Scheduling is set at the switch level. You cannot set this at the port level.

To change scheduling, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Queuing & Scheduling** tab.

   The Queuing & Scheduling tab is shown in Figure 61 on page 184.

   Note
   The Configure CoS Queues to Egress Queues section in the tab is explained in the previous procedure “Mapping CoS Priorities to Egress Queues” on page 184.

4. To select a scheduling method, click either **Strict Priority** or **Weighted Priority** in the Configure Egress Weights section of the tab. The default is Strict Priority.

   Skip the next step if you select Strict Priority. Queue weights do not apply to Strict Priority scheduling.

5. If you selected Weighted Priority, use the Queue # Weight fields to specify for each queue the number of packets you want a port to transmit before it goes to the next queue. The range is 1 to 15. For an example, refer to Table 5.

Table 5. Example of Weighted Round Robin Priority

Port Egress Queue	Maximum Number of Packets
Q0	1
Q1	1

Table 5. Example of Weighted Round Robin Priority (Continued)

Port Egress Queue	Maximum Number of Packets
Q2	1
Q3	5
Q4	5
Q5	5
Q6	15
Q7	15

Leaving the default value of 1 for each queue results in all egress queues being given the same priority.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the CoS Settings

To display the CoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Services**.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 62.

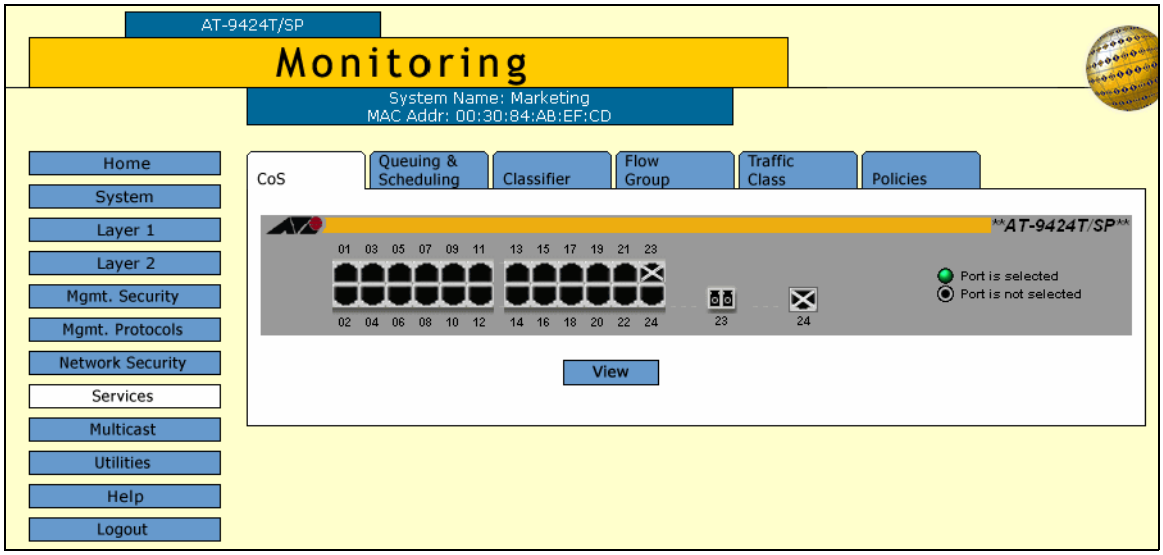

Figure 62. CoS Tab (Monitoring)

3. Click the port where you want to view the settings. You can select more than one port at a time. A selected port turns white. (To deselect a port, click it again.)

4. Click **View**.

The CoS Setting for Port page is shown in Figure 63.

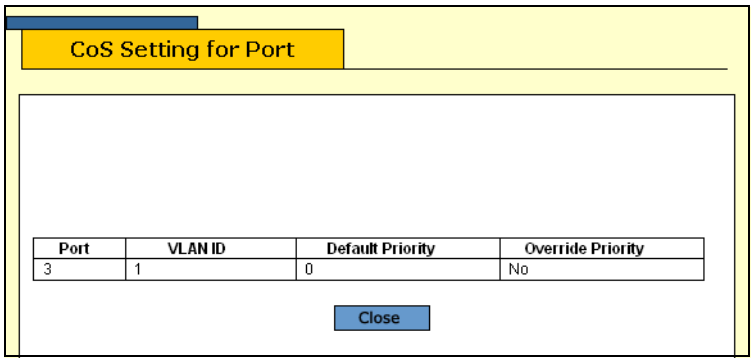

Figure 63. CoS Setting for Port Page

The CoS Setting for Port page displays a table that contains the following columns of information:

Port
The port number.

VLAN ID
The VLAN of which the port is a member.

Default Priority
The default priority level for this port.

Override Priority
Whether or not the priority level in tagged ports should be overridden.

5. Click **Close**.

Displaying the QoS Schedule

To display the QoS schedule, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 62 on page 188.

3. Select the **Queuing and Scheduling** tab.

   The Queuing and Scheduling tab is shown in Figure 64.

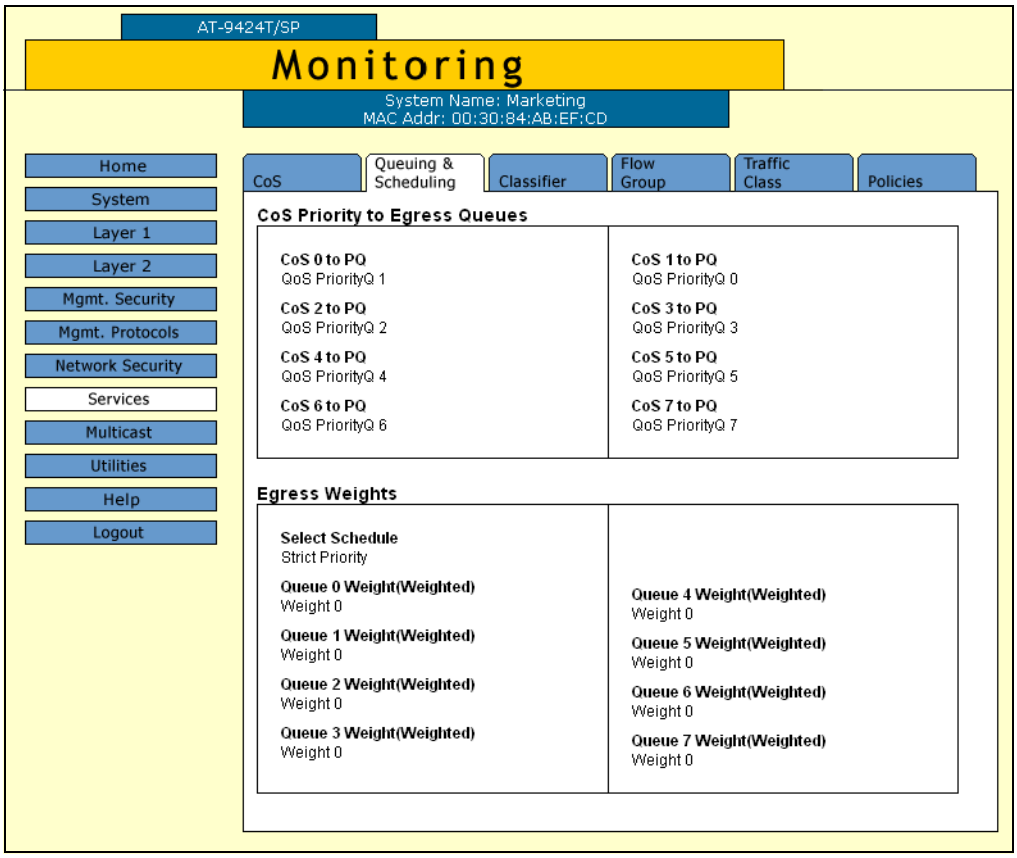

Figure 64. QoS Scheduling Tab (Monitoring)

The upper section displays the CoS priority to egress queue assignments. The lower section displays the egress weight settings.

Chapter 15

Quality of Service

This chapter contains instructions on how to configure Quality of Service (QoS). This chapter contains the following procedures:

- ❒ “Managing Flow Groups” on page 192
- ❒ “Managing Traffic Classes” on page 198
- ❒ “Managing Policies” on page 206

Note
For background information on QoS, refer to Chapter 17, “Quality of Service,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Managing Flow Groups

Flow groups are groups of classifiers that group together similar traffic flows. This section contains the following procedures:

- ❒ "Configuring Flow Groups," next
- ❒ "Modifying a Flow Group" on page 194
- ❒ "Deleting a Flow Group" on page 195
- ❒ "Displaying Flow Groups" on page 195

Configuring Flow Groups

To configure a flow group, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Flow Group** tab.

   The Flow Group tab is shown in Figure 65.

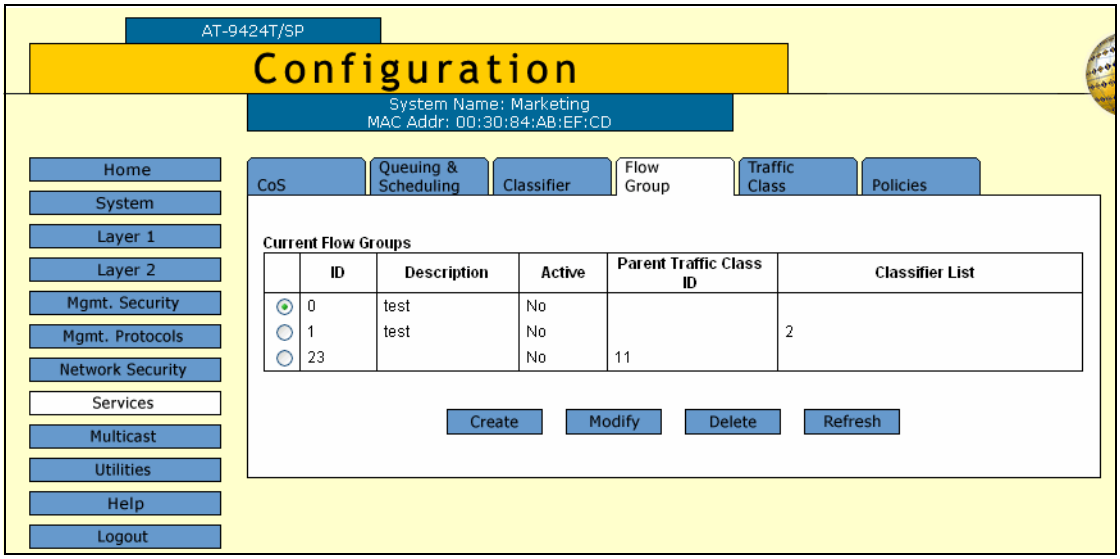

Figure 65. Flow Group Tab (Configuration)

4. Click **Create**.

   The Create Flow Group page opens, as shown in Figure 66.

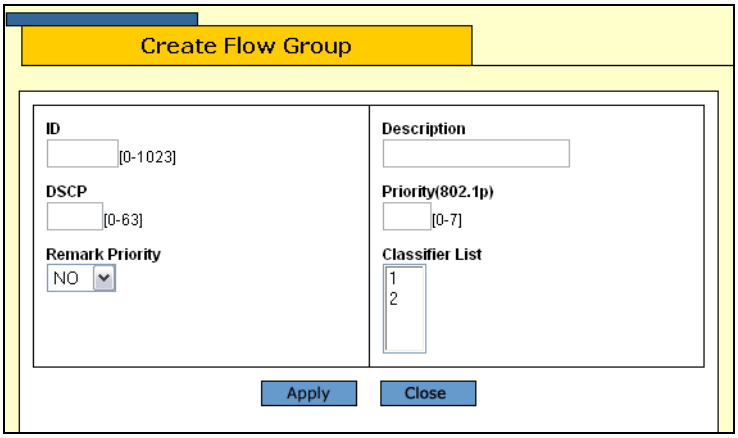

Figure 66. Create Flow Group Page

5. Configure the following parameters as necessary:

   ID
   Specifies the ID number for this flow group. The range is 0 to 1023.

   DSCP
   Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

   Remark Priority
   Replaces the user priority value in the packets with the new value specified in the Priority parameter.

   Description
   Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

   Priority (802.1p)
   Specifies a new user priority value for the packets. The range is 0 to 7.

   Classifier List
   The classifiers to be assigned to the policy. The specified classifiers must already exist. To select more than one classifier, use <Ctrl> click.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Flow Group

To modify a flow group, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the flow group you want to modify and click **Modify**.

   The Modify Flow Group page is displayed, as shown in Figure 67.

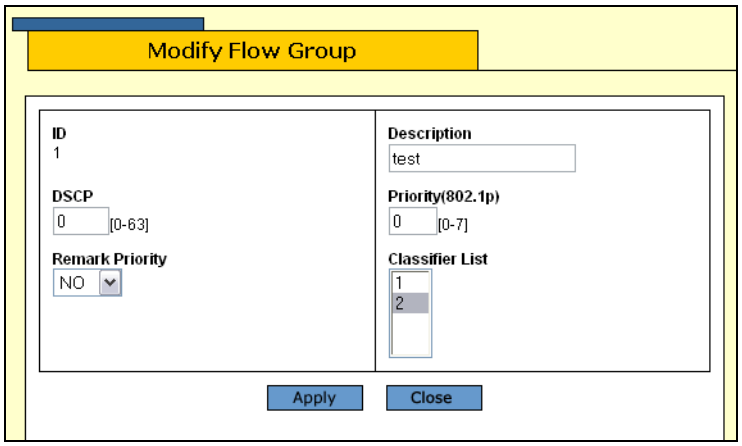

Figure 67. Modify Flow Group Page

4. Configure the following parameters as necessary:

   ID
   Specifies the ID number for this flow group. The range is 0 to 1023.

   DSCP
   Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

   Remark Priority
   Replaces the user priority value in the packets with the new value specified in the Priority parameter.

   Description
   Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

   Priority (802.1p)
   Specifies a new user priority value for the packets. The range is 0 to 7.

Classifier List
The classifiers to be assigned to the policy. The specified classifiers must already exist. To select more than one classifier, use <Ctrl> click.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Flow Group

To delete a flow group, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the flow group you want to delete and click **Delete**.

   The flow group is deleted from the list.

Displaying Flow Groups

To display the flow groups, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

   Note
   You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Services menu option.

2. From the Monitoring menu, select the **Services** option.

   The Services menu is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Flow Group** tab.

The Flow Group tab is shown in Figure 68.

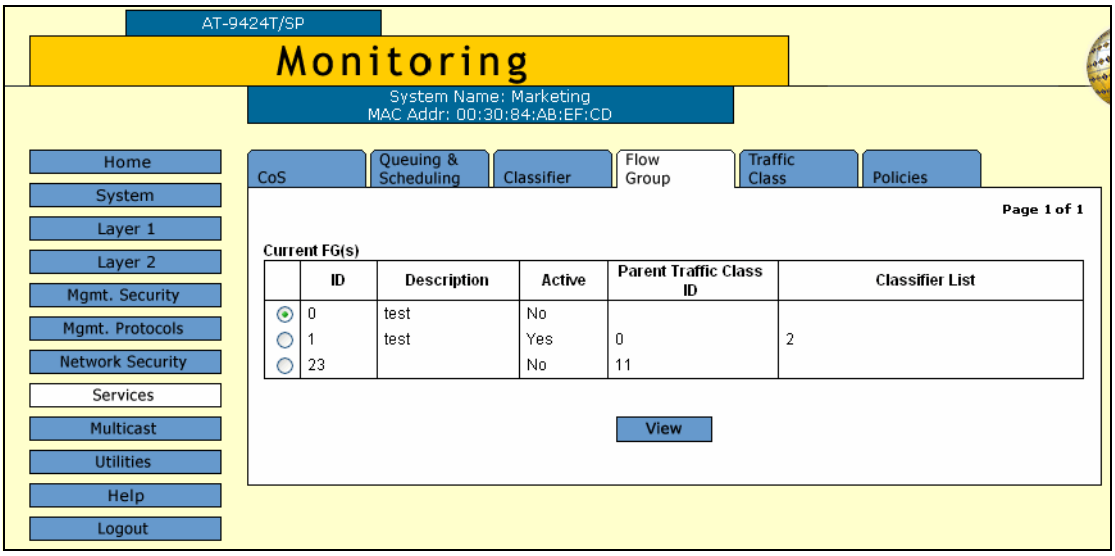

Figure 68. Flow Group Tab (Monitoring)

The Flow Group tab displays the currently configured flow groups in a table that contains the following columns of information:

ID
The ID number for this flow group.

Description
The flow group description.

Active
Whether or not the flow group is active.

Parent Traffic Class ID
The traffic class associated with this flow group. This information is for display only.

Classifier List
The classifiers assigned to the flow group.

4. To display detailed information about a flow group, select the flow group and click **View**.

The View Flow Group page is shown in Figure 69.

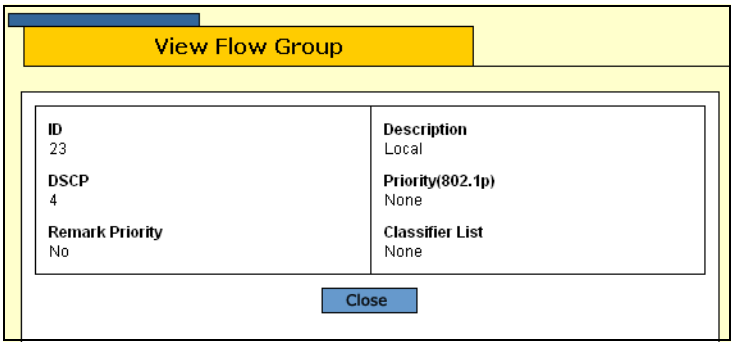

Figure 69. View Flow Group Page

The View Flow Group page displays the following information:

ID
The ID number for this flow group.

Description
The flow group description.

DSCP
The replacement value to write into the DSCP (TOS) field of the packets.

Priority
The new user priority value for the packets.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Classifier List
The classifiers assigned to the flow group.

5. Click **Close**.

Managing Traffic Classes

Traffic classes consist of a set of QoS parameters and a group of QoS flow groups. This section contains the following procedures:

- ❒ “Configuring Traffic Classes,” next
- ❒ “Modifying a Traffic Class” on page 200
- ❒ “Deleting a Traffic Class” on page 202
- ❒ “Displaying the Traffic Classes” on page 202

Configuring Traffic Classes

To configure a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 70.

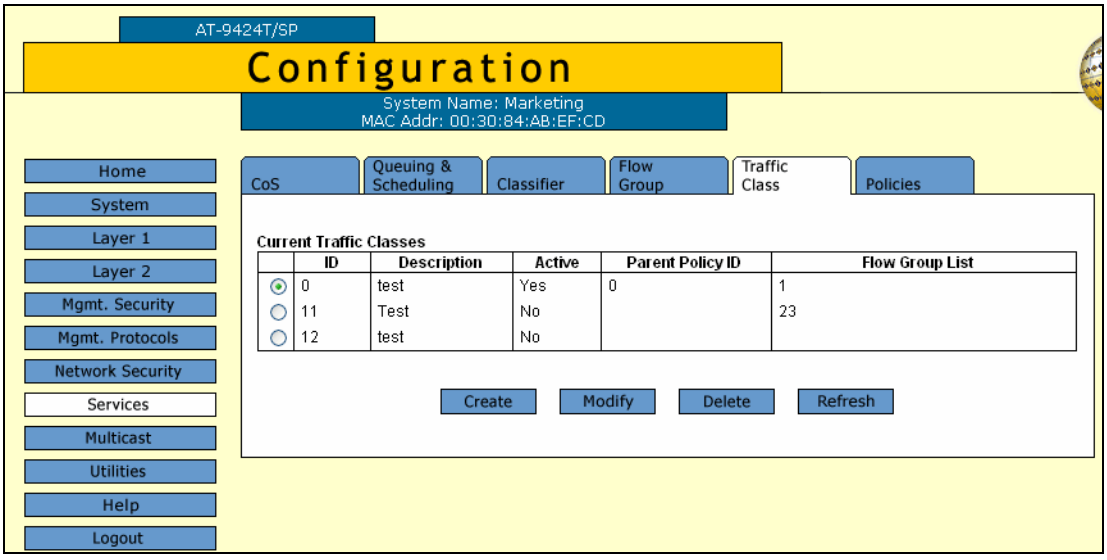

Figure 70. Traffic Class Tab

4. Click **Create**.

   The Create Traffic Class page is shown in Figure 71.

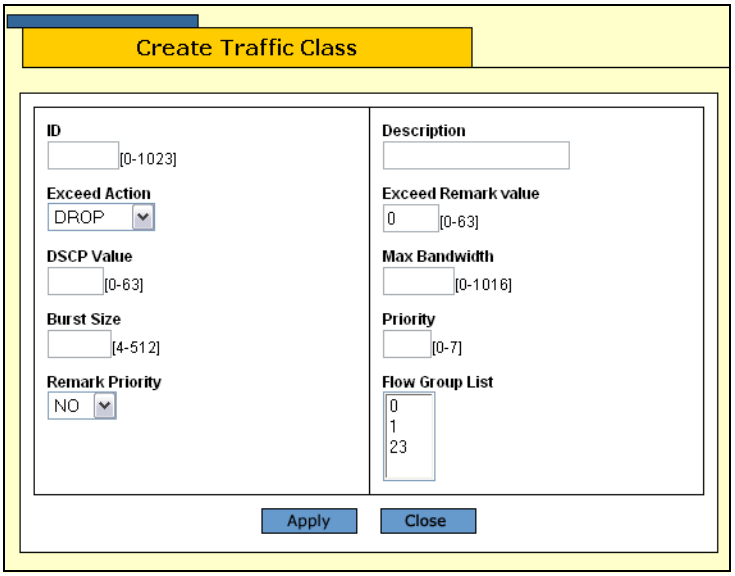

Figure 71. Create Traffic Class Page

5. Configure the following parameters:

   ID
   Specifies the ID number for this traffic class. The range is 0 to 1023.

   Exceed Action
   Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth specified by the Max Bandwidth parameter. The possible options are drop and remark.

   DSCP
   Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

   Burst Size
   Specifies the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. You must also specify the Max Bandwidth.

   Remark Priority
   Replaces the user priority value in the packets with the new value specified in the Priority parameter.

   Description
   Specifies the traffic class description. A description can be up to 15 alphanumeric characters, including spaces.

Exceed Remark Value
Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The default is 0.

Max Bandwidth
Specifies the maximum bandwidth available for the traffic class. The range is 0 to 1016 Mbps. If you set this parameter to 0 (zero), all traffic that matches that traffic class is dropped.

Priority
Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7 with 0 (zero) as the lowest priority.

Flow Group List
The flow groups assigned to this traffic class. Use <Ctrl> click to select more than one.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Traffic Class

To modify a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 70 on page 198

4. Select the traffic class you want to modify and click **Modify**.

The Modify Traffic Class page is shown in Figure 72.

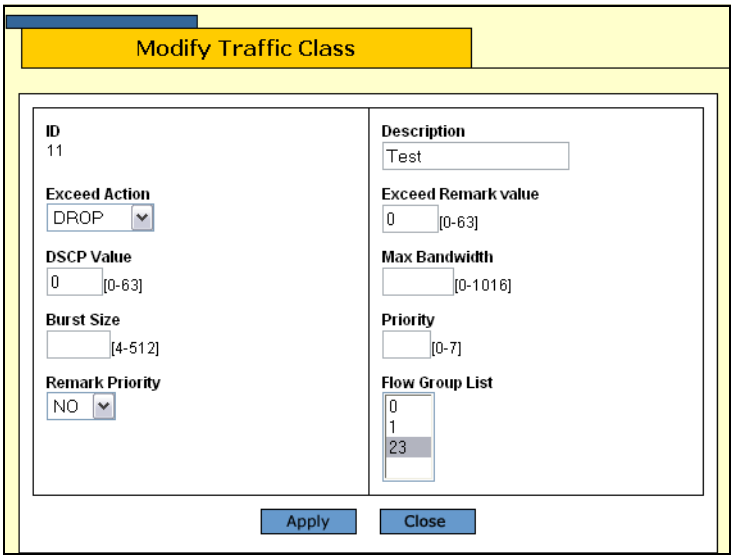

Figure 72. Modify Traffic Class Page

5. Configure the following parameters as necessary:

ID
Specifies the ID number for this traffic class. The range is 0 to 1023.

Exceed Action
Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth specified by the Max Bandwidth parameter. The possible options are drop and remark.

DSCP
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Burst Size
Specifies the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. You must also specify the Max Bandwidth.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description
Specifies the traffic class description. A description can be up to 15 alphanumeric characters, including spaces.

Exceed Remark Value
Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The default is 0.

Max Bandwidth
Specifies the maximum bandwidth available for the traffic class. The range is 0 to 1016 Mbps. If you set this parameter to 0 (zero), all traffic that matches that traffic class is dropped.

Priority
Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7 with 0 (zero) as the lowest priority.

Flow Group List
The flow groups assigned to this traffic class. Use <Ctrl> click to select more than one.

6. Click Apply.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Traffic Class

To delete a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 70 on page 198

4. Select the traffic class you want to delete and click **Delete**.

   The traffic class is deleted from the list.

Displaying the Traffic Classes

To display the traffic classes, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Services**.

   The Services menu is displayed with the CoS tab selected by default, as shown in Figure 62 on page 188.

3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 73.

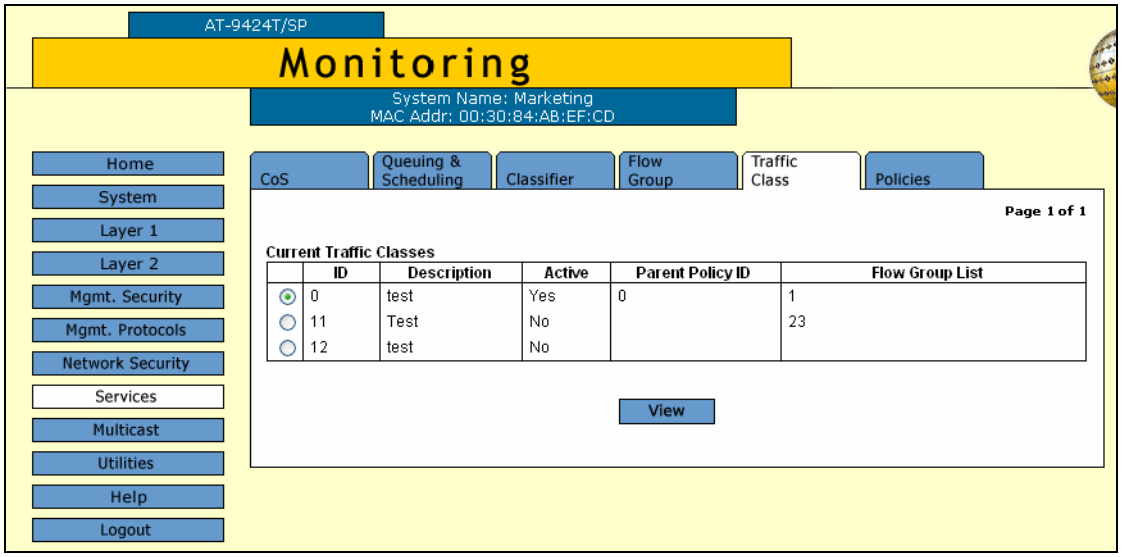

Figure 73. Traffic Class Tab (Monitoring)

The Traffic Class tab displays the currently configured flow groups in a table that contains the following columns of information:

ID
The ID of the traffic class.

Description
A description of the traffic class.

Active
Whether or not this traffic class is active on the switch.

Parent Policy ID
The policy associated with this traffic class. This information is for display only.

Flow Group List
The flow groups assigned to this traffic class.

4. To display detailed information about a traffic class, select the traffic class and click **View**.

The View Traffic Class page is shown in Figure 74.

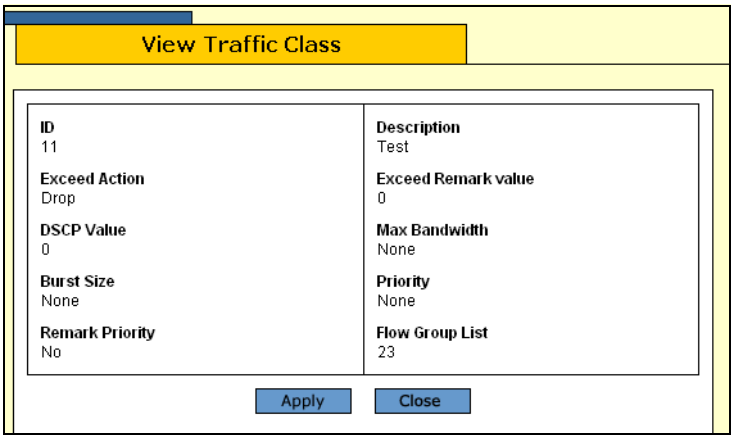

Figure 74. View Traffic Class Page

The View Traffic Class page displays the following information:

ID
The ID of the traffic class.

Exceed Action
The action to be taken if the traffic of the traffic class exceeds the maximum bandwidth specified by the Max Bandwidth parameter.

DSCP Value
The replacement value to write into the DSCP (TOS) field of the packets.

Burst Size
The size of a token bucket for the traffic class.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description
A description of the traffic class.

Exceed Remark Value
The DSCP replacement value for traffic that exceeds the maximum bandwidth.

Max Bandwidth
The maximum bandwidth available for the traffic class.

Priority
The priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned.

Flow Group List
The flow groups assigned to this traffic class.

5. Click **Close**.

Managing Policies

QoS policies consist of a collection of user-defined traffic classes. This section contains the following procedures:

- ❒ “Configuring a Policy,” next
- ❒ “Modifying a Policy” on page 208
- ❒ “Deleting a Policy” on page 210
- ❒ “Displaying Policies” on page 210

Configuring a Policy

To configure a policy, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Policies** tab.

   The Policies tab is shown in Figure 75.

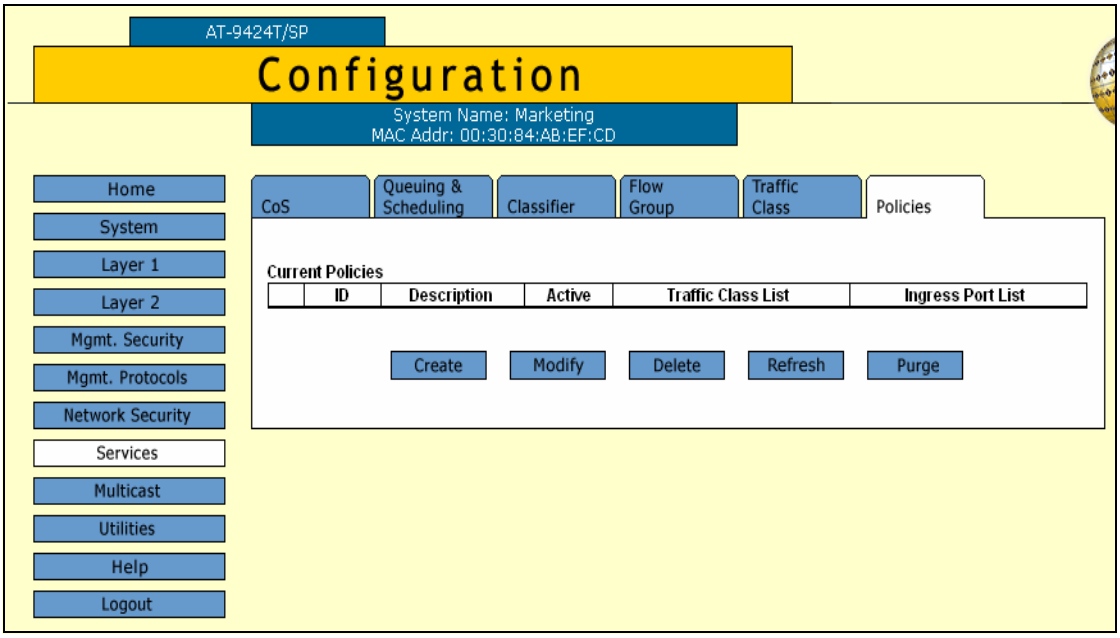

Figure 75. Policies Tab (Configuration)

The Policies tab displays the existing policies in a table that contains the following columns of information:

ID
The ID of the policy.

Description
A description of the policy.

Active
Whether or not this policy is active on the switch.

Traffic Class List
The traffic classes assigned to the policy.

Ingress Port List
The ingress ports to which the policy is assigned.

4. Click **Create**.

   The Create Policy page opens, as shown in Figure 76.

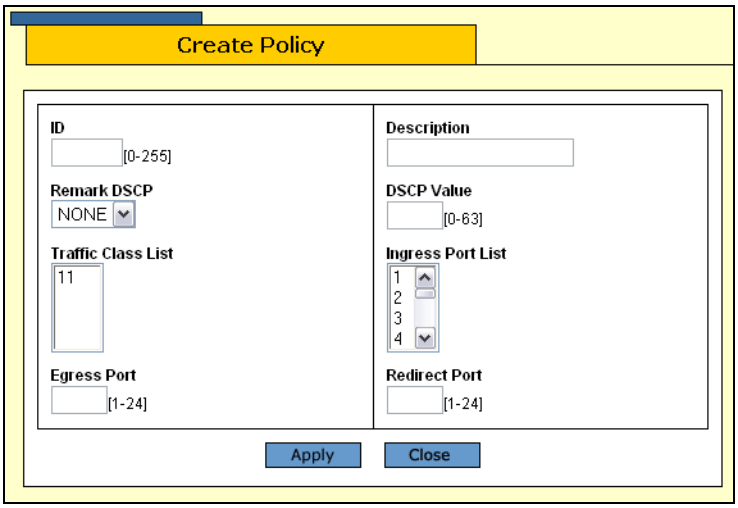

Figure 76. Create Policy Page

5. Configure the following parameters as necessary:

   ID
   Specifies the ID number for this policy. The range is 0 to 255.

   Description
   Specifies the policy description. A description can be up to 15 alphanumeric characters, including spaces.

   Remark DSCP
   Specifies the conditions under which the ingress DSCP value is overwritten. Select one of the following options from the list:

None - Disables this function.

All - All packets are remarked.

DSCP Value
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Traffic Class List
Specifies the traffic classes to be assigned to the policy. The traffic classes must already exist. Select the classes from the list. To select more than one, use <Ctrl> click.

Ingress Port List
Specifies the ingress ports to which the policy is to be assigned. Select the ports from the list. To select more than one, use <Ctrl> click. A port can be an ingress port of only one policy at a time.

Egress Port
Specifies the egress port to which the policy is to be assigned. A port can be an egress port of only one policy at a time.

Redirect Port
Specifies the port to which the classified traffic from the ingress ports is redirected.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Policy

To modify a policy, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Policies** tab.

   The Policies tab is shown in Figure 75 on page 206.

4. Select a policy from the list and click **Modify**.

The Modify Policy page is shown in Figure 77.

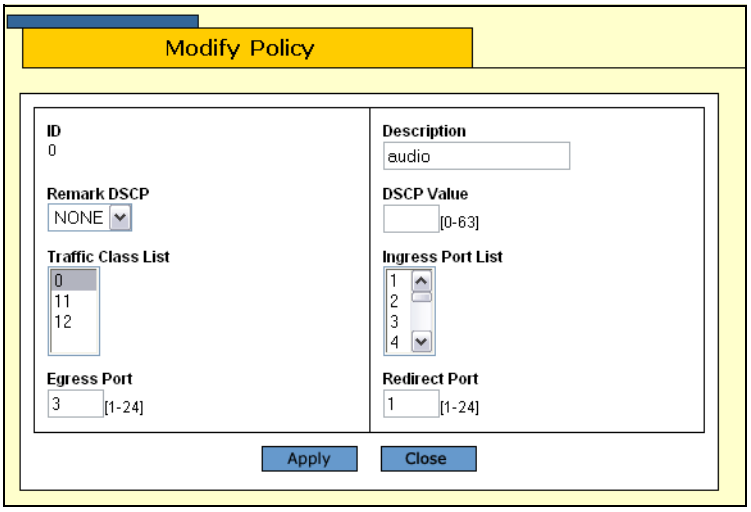

Figure 77. Modify Policy Page

5. Modify the following parameters as necessary:

ID
Specifies the ID number for this policy. The range is 0 to 255.

Description
Specifies the policy description. A description can be up to 15 alphanumeric characters, including spaces.

Remark DSCP
Specifies the conditions under which the ingress DSCP value is overwritten. Select one of the following options from the list:

None - Disables this function.

All - All packets are remarked.

DSCP Value
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Traffic Class List
Specifies the traffic classes to be assigned to the policy. The traffic classes must already exist. Select the classes from the list. To select more than one, use <Ctrl> click.

Ingress Port List
Specifies the ingress ports to which the policy is to be assigned. Select the ports from the list. To select more than one, use <Ctrl> click. A port can be an ingress port of only one policy at a time.

Egress Port
Specifies the egress port to which the policy is to be assigned. A port can be an egress port of only one policy at a time.

Redirect Port
Specifies the port to which the classified traffic from the ingress ports is redirected.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Policy

To delete a policy, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 59 on page 182.

3. Select the **Policies** tab.

   The Policies tab is shown in Figure 75 on page 206.

4. Do one of the following:

   - Select a policy from the list and click **Delete**.
   - Click **Purge** to delete all the policies

Displaying Policies

To display the policies, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Services**.

   The Services menu is displayed with the CoS tab selected by default, as shown in Figure 62 on page 188.

3. Select the **Policies** tab.

The Policies tab is shown in Figure 78.

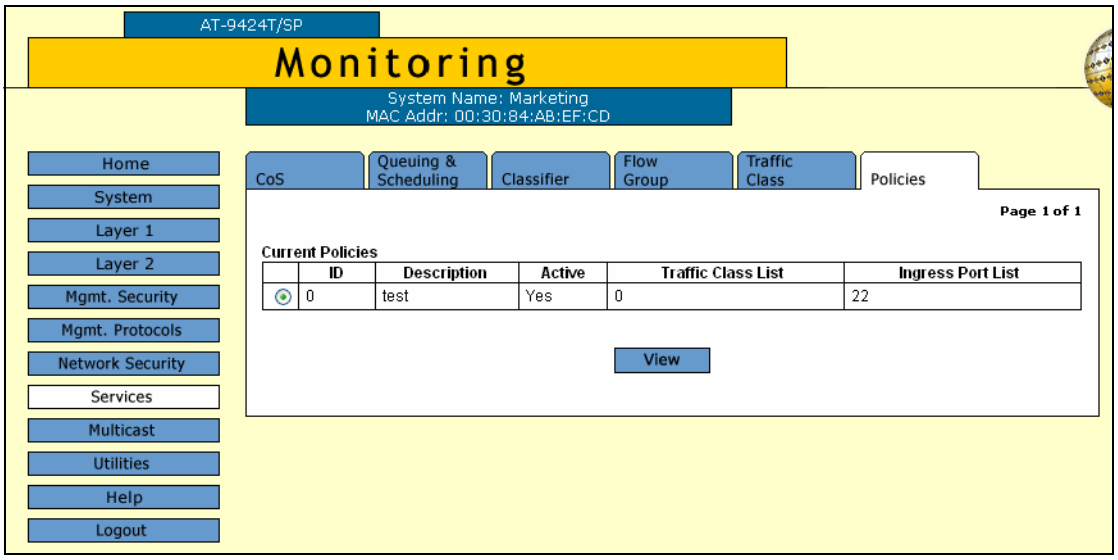

Figure 78. Policies Tab (Monitoring)

The Policies tab displays the existing policies in a table that contains the following columns of information:

ID
The ID of the policy.

Description
A description of the policy.

Active
Whether or not this policy is active on the switch.

Traffic Class List
The traffic classes assigned to the policy.

Ingress Port List
The ingress ports to which the policy is assigned.

4. To view the details of a specific policy, select the policy and click View.

The View Policy page is shown in Figure 79.

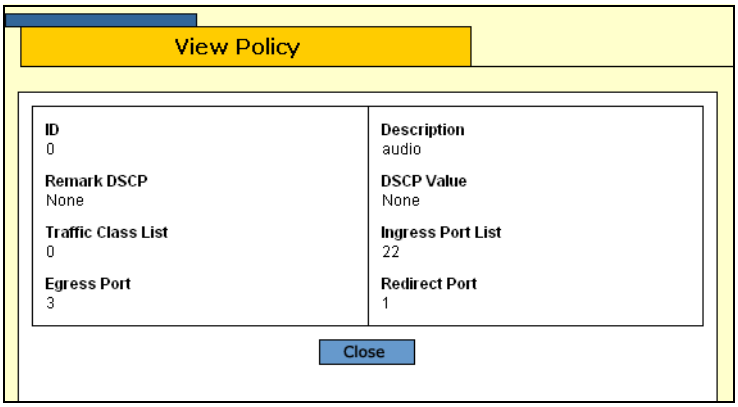

Figure 79. View Policy Page

The View Policy page contains the following information:

ID
The ID of the policy.

Description
A description of the policy.

Remark DSCP
The conditions under which the ingress DSCP value is overwritten.

DSCP Value
A replacement value to write into the DSCP (TOS) field of the packets.

Traffic Class List
The traffic classes to be assigned to the policy.

Ingress Port List
The ingress ports to which the policy is to be assigned.

Egress Port
The egress port to which the policy is to be assigned.

Redirect Port
The port to which the classified traffic from the ingress ports is redirected.

5. Click **Close**.

Chapter 16

Denial of Service Defense

This chapter contains instructions on how to configure the Denial of Service defense feature on the switch. The sections include:

- ❒ “Configuring Denial of Service Defense” on page 214
- ❒ “Displaying the DoS Settings” on page 217

Note
For background information on denial of service defense, refer to Chapter 18, “Denial of Service Defense,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring Denial of Service Defense

To configure the ports on the switch for Denial of Service attack defense, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 158 on page 392.

3. Select the **DoS** tab.

   The DoS tab is shown in Figure 80.

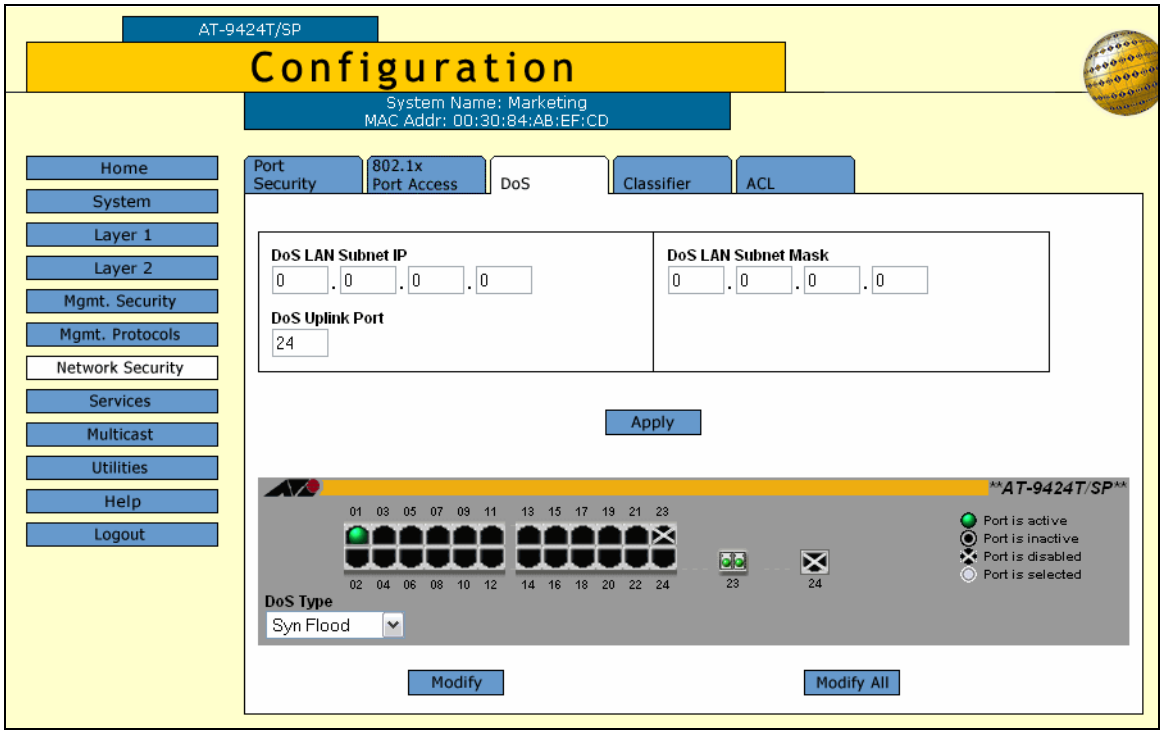

Figure 80. DoS Tab (Configuration)

4. If you are implementing the SMURF or Land defense, you must provide an IP address and mask for your LAN. To do this, complete the following procedure: Otherwise, skip ahead to Step 5.

   a. In the DoS LAN Subnet IP field, enter the IP address of one of the devices connected to the switch, preferably the lowest IP address.

b. In the DoS Subnet Mask field, enter the LAN's mask. enter the mask. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to 149.11.11.50. The mask would be 0.0.0.63.

c. If you are activating the Land defense, in the DoS Uplink Port field enter the number of the port connected to the device (e.g., DSL router) that leads outside your network. You can specify only one uplink port.

5. Click the ports in the switch image where you want to enable or disable a defense mechanism.

6. Using the DoS Type list, select the type of denial of service attack you want to either enable or disable on the ports. The possible selections are:

   - Syn Flood attack
   - Smurf attack
   - Land attack
   - Tear drop attack
   - Ping of death attack
   - IP Options

7. Click **Modify**. To configure all the ports, click **Modify All**.

   The DoS Configuration for Ports page opens. The page shown in Figure 81 is for IP Options.

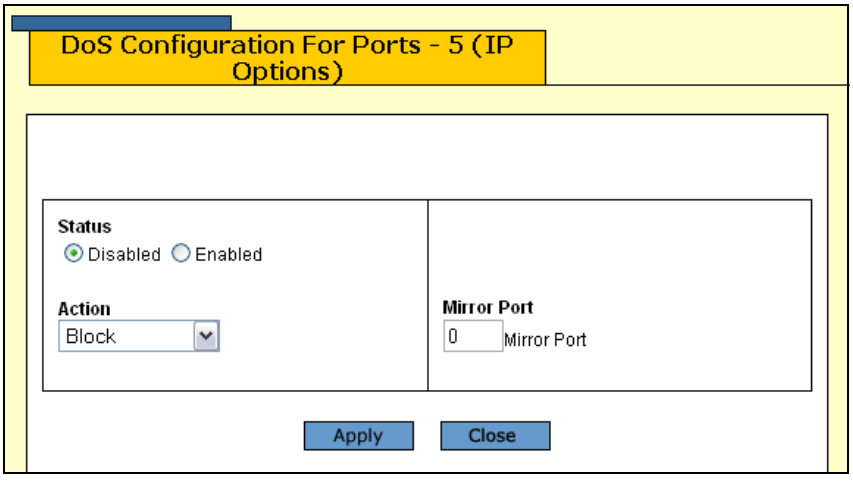

Figure 81. DoS Configuration for Ports Page

8. Configure the following parameters as necessary:

Status
Click Enable or Disable to enable or disable DoS on the selected ports.

Action
The action a port takes when an intruder packet is received. Although five possible selections are shown in the Action list box, they all do the same thing: block the packet, record the event, and drop the packet. This option applies only to the IP Options defense.

Mirror Port
This option applies to the Land, Tear Drop, Ping of Death, and IP Options. You can use this option to copy offending traffic to another port on the switch. You can specify only one mirror port. Specifying a mirror port is not required.

9. Click **Apply**.

   The defense is immediately activated on the ports.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the DoS Settings

To display the DoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Network Security**.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 160 on page 395.

3. Select the **DoS** tab.

   The DoS tab is shown in Figure 82.

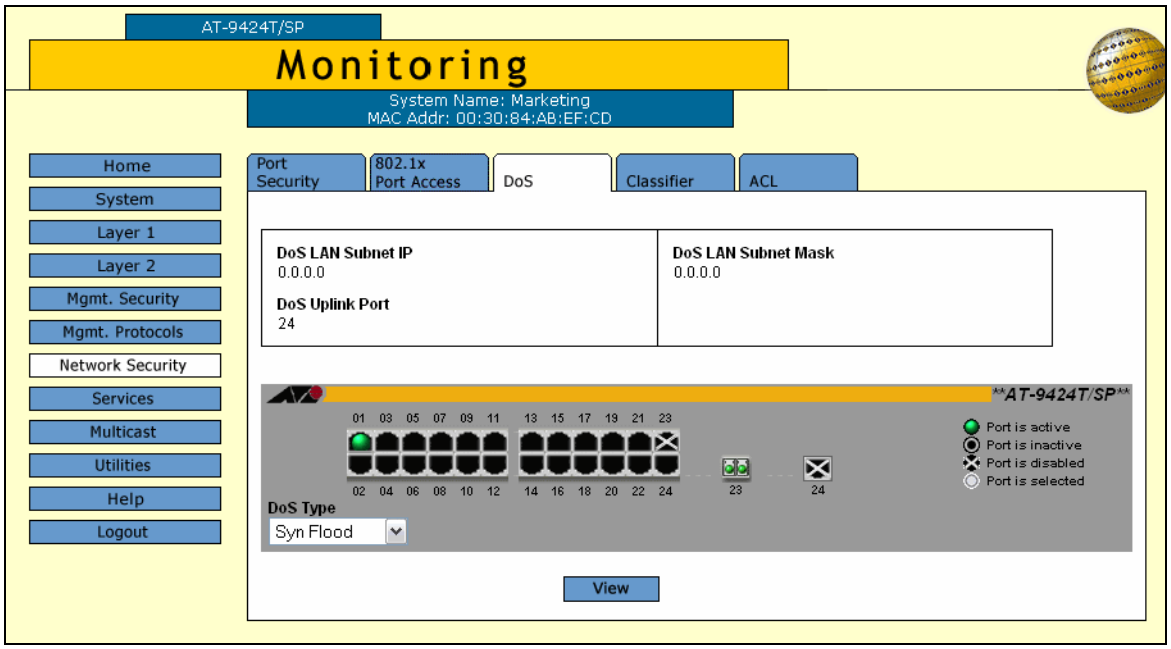

Figure 82. DoS Tab (Monitoring)

4. Click the port whose DoS settings you want to view. You can select more than one port at a time.

5. Using the DoS Type list, select the type of denial of service defense whose settings you want to view.

6. Click **View**.

The DoS Monitor for Port page opens, as shown in Figure 83.

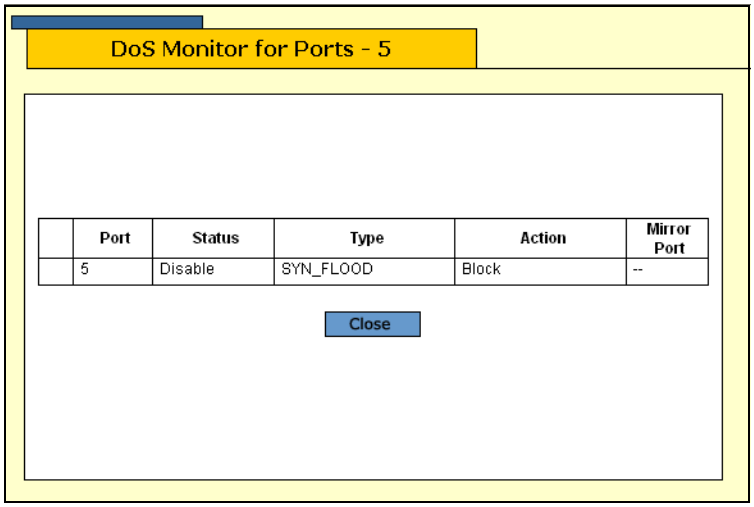

Figure 83. DoS Monitor for Ports Page

The page displays a table that contains the following columns of information:

Port
The port number.

Status
Whether DoS is enabled or disabled on the port.

Type
The type of DoS prevention.

Action
The action a port takes when an intruder packet is received. Although five possible selections are shown in the Action list box, they all do the same thing: block the packet, record the event, and drop the packet. This column is only displayed for the IP Options defense.

Mirror Port
The port on the switch to which offending traffic is copied.

Chapter 17

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. The sections in the chapter include:

- ❒ “Configuring IGMP Snooping” on page 220
- ❒ “Displaying a List of Host Nodes” on page 223
- ❒ “Displaying a List of Multicast Routers” on page 226

Note
For background information, refer to Chapter 19, “IGMP Snooping,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring IGMP Snooping

To configure IGMP snooping, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Multicast** option.

   The Multicast page is displayed with the **IGMP** tab selected by default, as shown in Figure 84.

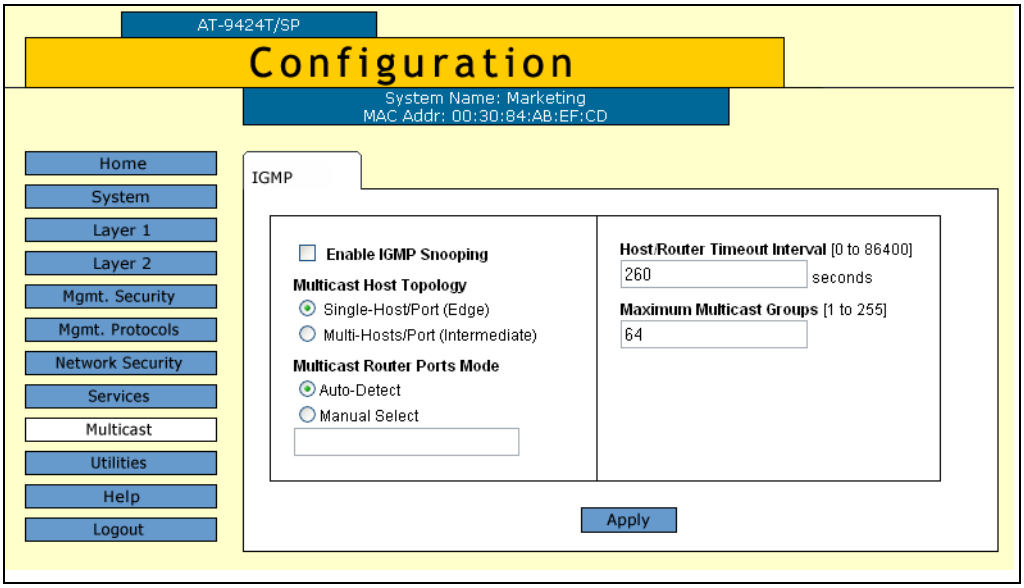

Figure 84. IGMP Tab (Configuration)

3. Configure the following parameters as necessary.

   Enable IGMP Snooping Status
   Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

   Multicast Host Topology
   Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

   The Edge (Single-Host/Port) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending

reports and times out. The switch forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Intermediate (Multi-Host) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.

Multicast Router Ports Mode
Specifies whether the router ports are determined automatically or if you enter them manually. If you want the switch to determine the ports automatically, select Auto-Detect, which is the default. To enter them yourself, click Manual Select and enter the ports in the field.

Host/Router Timeout Interval
Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

Maximum Multicast Groups
Specifies the maximum number of multicast groups the switch learns. The range is 1 to 255 groups. The default is 64 multicast groups.

This setting is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

4. Click **Apply**.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying a List of Host Nodes

You can use the AT-S63 management software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes.

To view host nodes, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Multicast** option.

   The Multicast page is displayed with the IGMP tab as shown in Figure 85.

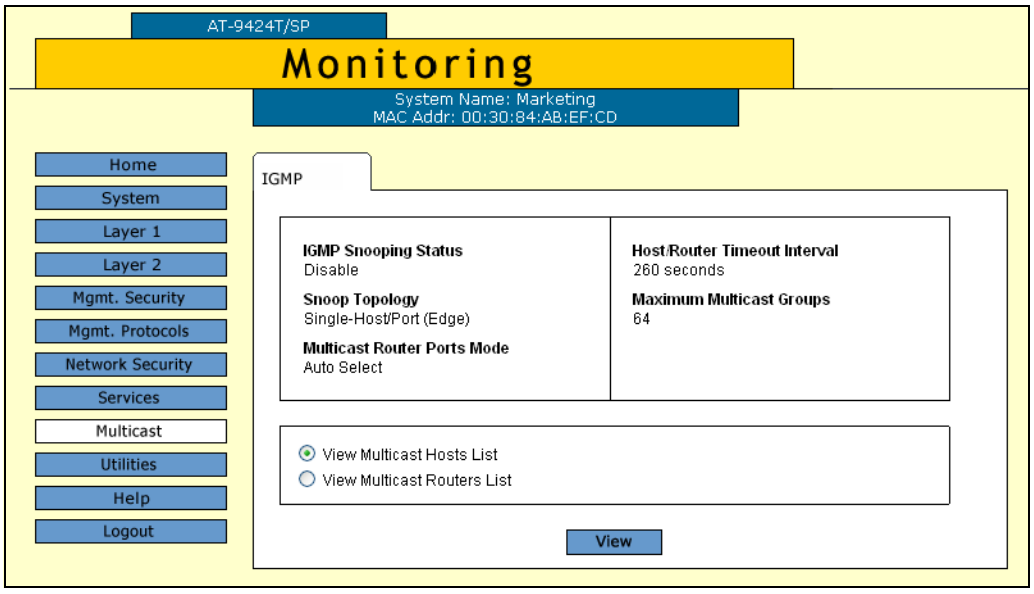

Figure 85. IGMP Tab (Monitoring)

The IGMP tab provides the following information:

Enable IGMP Snooping Status
The IGMP snooping status on the switch. Possible settings are Enabled and Disabled

Snoop Topology
Whether there is only one host node per switch port or multiple host nodes per port. The possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

Multicast Router Ports Mode
How the router ports are determined. The possible settings are:

Auto-Detect - The switch determines the ports automatically.

Port number - The selected router ports.

Host/Router Timeout Interval
The time period in seconds after which the switch determines that a host node has become inactive.

Maximum Multicast Groups
The maximum number of multicast groups the switch learns.

3. To view the multicast addresses and the host nodes, click **View Multicast Hosts List** and then click **View**.

   The View Multicast Hosts List is shown in Figure 86.

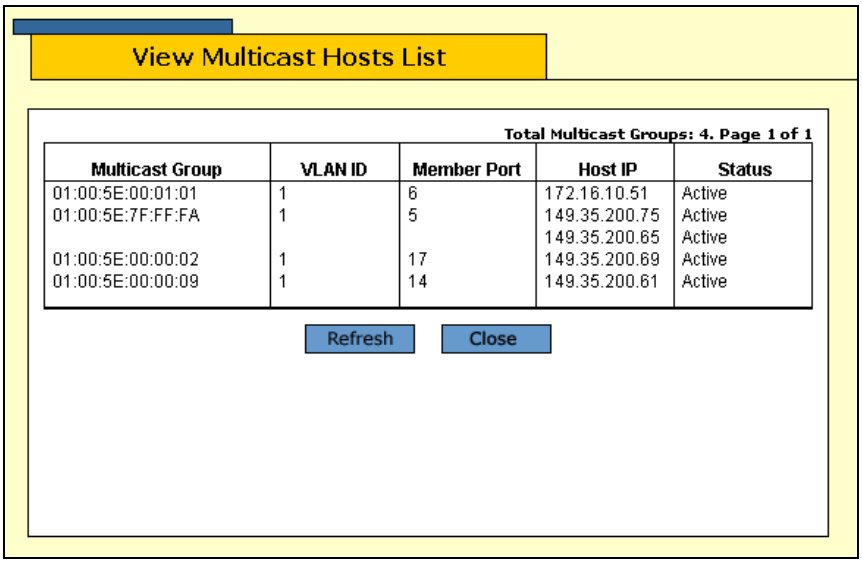

Figure 86. View Multicast Hosts List Page

The View Multicast Hosts List page displays a table that contains the following columns of information:

Multicast Group
The multicast address of the group.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Member Port
The port(s) on the switch to which one or more host nodes of the multicast group are connected.

Host IP
The IP address(es) of the host node(s) connected to the port.

Status
Indicates IGMP group status of the port. The possible settings are:

Active - The port is active in the IGMP group.

Left Group - The port is not active in the IGMP group.

Displaying a List of Multicast Routers

To view multicast routers, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **IGMP** tab.

   The IGMP tab is shown in Figure 85 on page 223.

3. To view the multicast routers, click **View Multicast Router List** and then click **View**.

   The View Multicast Routers List is shown in Figure 87.

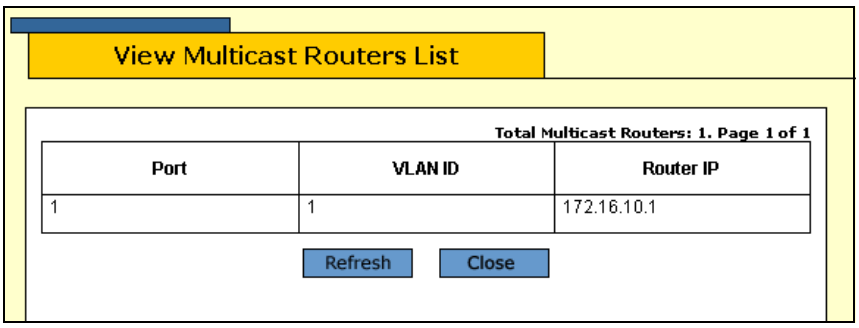

Figure 87. View Multicast Routers List Page

The View Multicast Routers List page displays a table that contains the following columns of information:

Port
The port on the switch where the multicast router is connected.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the port on the router.

If the routers are static routers (specified with the Manual Select option on the Configuration IGMP page), then the View Multicast Routers List page opens, as shown in Figure 88 on page 227.

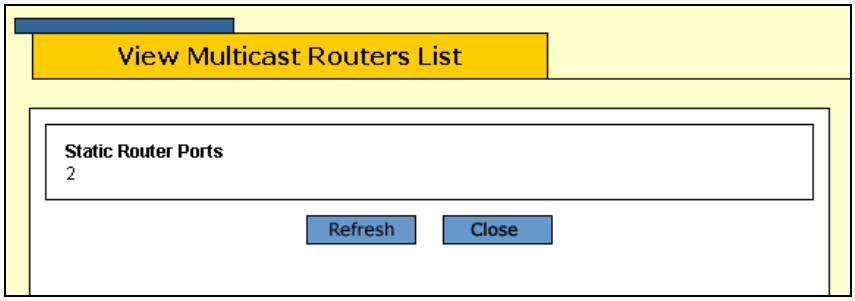

Figure 88. View (Static) Multicast Routers List Page

Section III
SNMPv3

The chapter in this section contains the procedures for configuring SNMPv3. The chapter is:

- Chapter 18, “SNMPv3” on page 231

Chapter 18
SNMPv3

This chapter provides the following procedures for configuring SNMPv3 parameters using a web browser management session:

- ❒ “Configuring the SNMPv3 Protocol” on page 232
- ❒ “Enabling or Disabling SNMP Management” on page 233
- ❒ “Configuring the SNMPv3 User Table” on page 236
- ❒ “Configuring the SNMPv3 View Table” on page 244
- ❒ “Configuring the SNMPv3 Access Table” on page 250
- ❒ “Configuring the SNMPv3 SecurityToGroup Table” on page 257
- ❒ “Configuring the SNMPv3 Notify Table” on page 263
- ❒ “Configuring the SNMPv3 Target Address Table” on page 268
- ❒ “Configuring the SNMPv3 Target Parameters Table” on page 275
- ❒ “Configuring the SNMPv3 Community Table” on page 282
- ❒ “Displaying SNMPv3 Tables” on page 288

Note
For background information on SNMPv3, refer to Chapter 22, “SNMPv3,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to first enable SNMP access on the switch. Then you configure the SNMPv3 tables. See the following procedures:

- ❒ “Enabling or Disabling SNMP Management” on page 233
- ❒ “Configuring the SNMPv3 User Table” on page 236
- ❒ “Configuring the SNMPv3 View Table” on page 244
- ❒ “Configuring the SNMPv3 Access Table” on page 250
- ❒ “Configuring the SNMPv3 SecurityToGroup Table” on page 257
- ❒ “Configuring the SNMPv3 Notify Table” on page 263
- ❒ “Configuring the SNMPv3 Target Address Table” on page 268
- ❒ “Configuring the SNMPv3 Target Parameters Table” on page 275
- ❒ “Configuring the SNMPv3 Community Table” on page 282

Note
Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

Enabling or Disabling SNMP Management

In order to allow an SNMP manager or host to access the switch you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a login attempt from an unauthenticated user, you need to enable authentication failure traps. This section provides a procedure to accomplish both of these tasks.

To enable SNMP access and authentication failure traps, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 89.

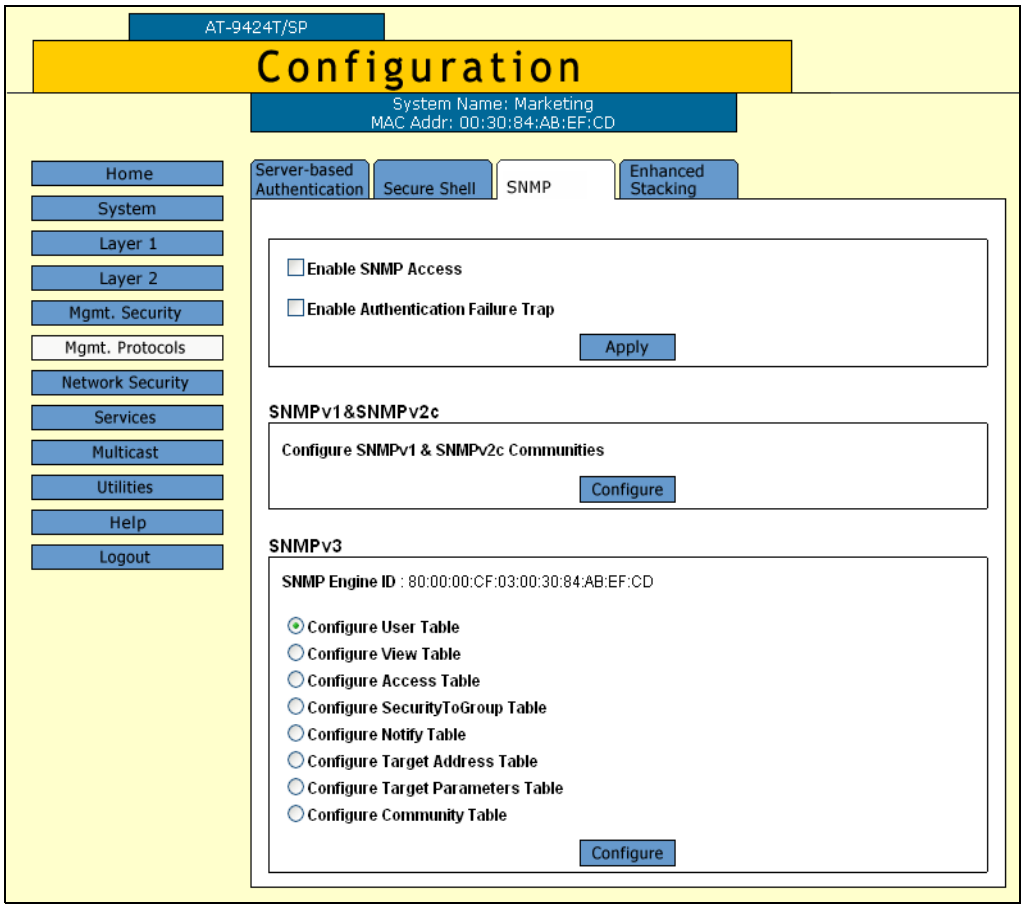

Figure 89. SNMP Tab (Configuration)

4. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.

   Use this parameter to enable the switch to be remotely managed with an SNMP application program.

   Note
   If the Enable SNMP Access check box is not checked, the switch cannot be managed through SNMP. This is the default.

5. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 User Table

You can create, delete, and modify an SNMPv3 User Table entry. See the following procedures:

- “Creating a User Table Entry” on page 236
- “Deleting a User Table Entry” on page 239
- “Modifying a User Table Entry” on page 240

For reference information about the SNMPv3 User Table, see Chapter 22, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a User Table Entry

To create an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 89 on page 234.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 90.

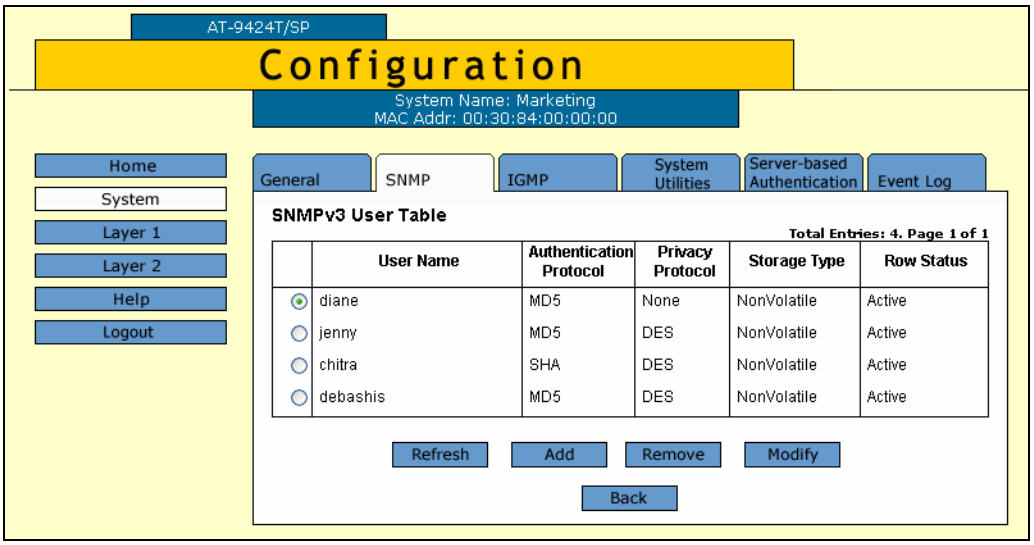

Figure 90. SNMPv3 User Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 User page is shown in Figure 91.

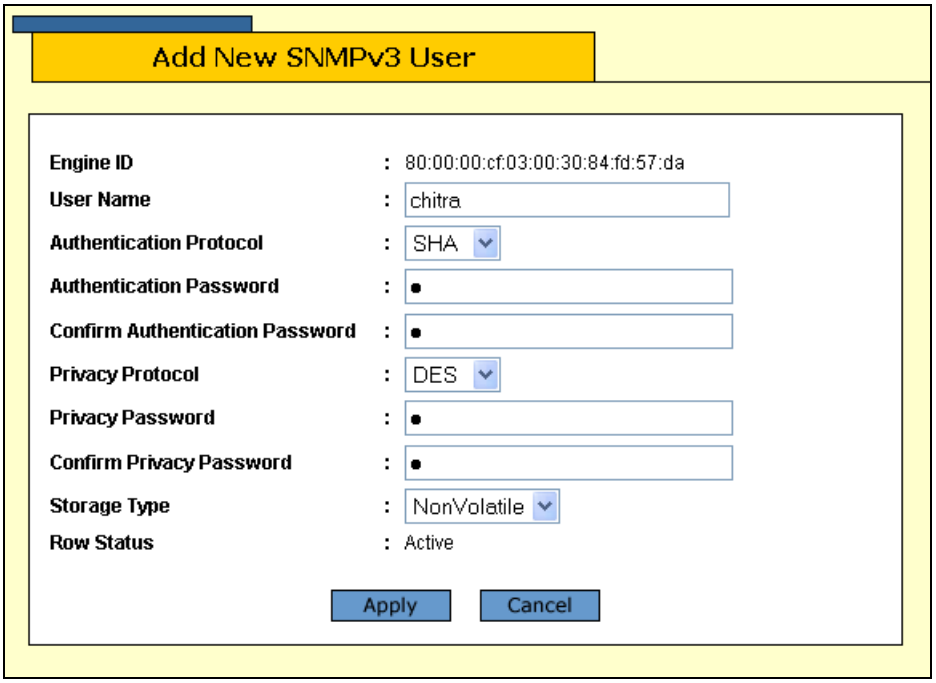

Figure 91. Add New SNMPv3 User Page

5. In the User Name field, enter a name, or logon id, that consists of up to 32 alphanumeric characters

6. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

   Select one of the following:

   MD5
   This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

   SHA
   This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

   None
   This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

   Note
   You may want to assign NONE to a super user.

7. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.

8. In the Confirm Authentication Password field, re-enter the authentication password.

   Note
   If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

   Note
   You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

9. In the Privacy Protocol field, enter one of the following options:

   DES
   Select this value to make the DES privacy (or encryption) protocol the

privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

None
Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

10. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.

11. In the Confirm Privacy Password field, re-enter the privacy password.

12. In the Storage Type field, enter one of the following storage options for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the User Table. After making changes to an User Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the User Table. After making changes to an User Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

    Note
    The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 User Table.

14. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a User Table Entry

To delete an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

   The SNMPv3 User Table tab is shown in Figure 90 on page 237.

4. Click the button next to the User Table entry that you want to delete and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a User Table Entry

To modify an entry SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

   The SNMPv3 User Table tab is shown in Figure 90 on page 237.

4. Click the button next to the SNMPv3 user that you want to change and then click **Modify**.

The Modify SNMPv3 User page is shown in Figure 92.

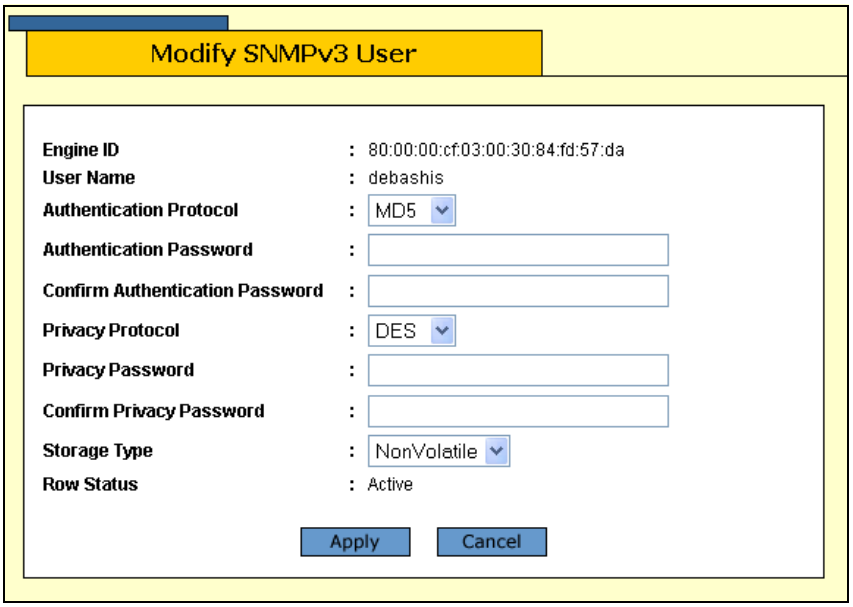

Figure 92. Modify SNMPv3 User Page

5. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

   Select one of the following:

   MD5
   This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

   SHA
   This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

   None
   This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note
You may want to assign NONE to a super user.

6. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.

7. In the Confirm Authentication Password field, re-enter the authentication password.

Note
If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

Note
You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

8. In the Privacy Protocol field, enter one of the following options:

   DES
   Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

   None
   Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

9. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.

10. In the Confirm Privacy Password field, re-enter the privacy password.

11. In the Storage Type field, enter one of the following storage options for this User Table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table

entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

12. Click **Apply** to update the SNMPv3 User Table.
13. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 View Table

You can create, delete, and modify an SNMPv3 View Table entry. See the following procedures:

- “Creating a View Table Entry” on page 244
- “Deleting a View Table Entry” on page 247
- “Modifying a View Table Entry” on page 247

For reference information about the SNMPv3 View Table, see Chapter 22, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a View Table Entry

To create an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 93.

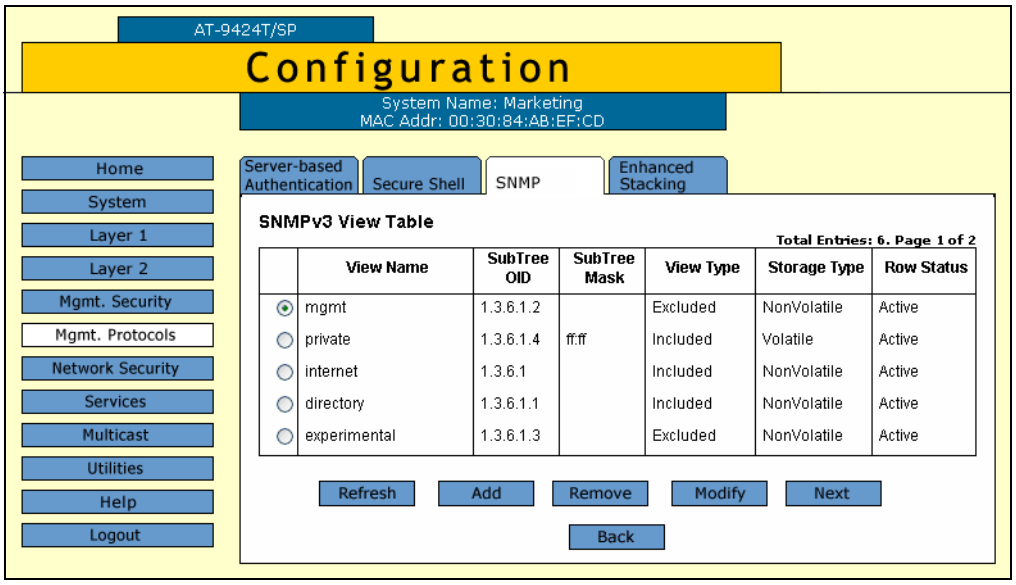

Figure 93. SNMPv3 View Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 View page is shown in Figure 94.

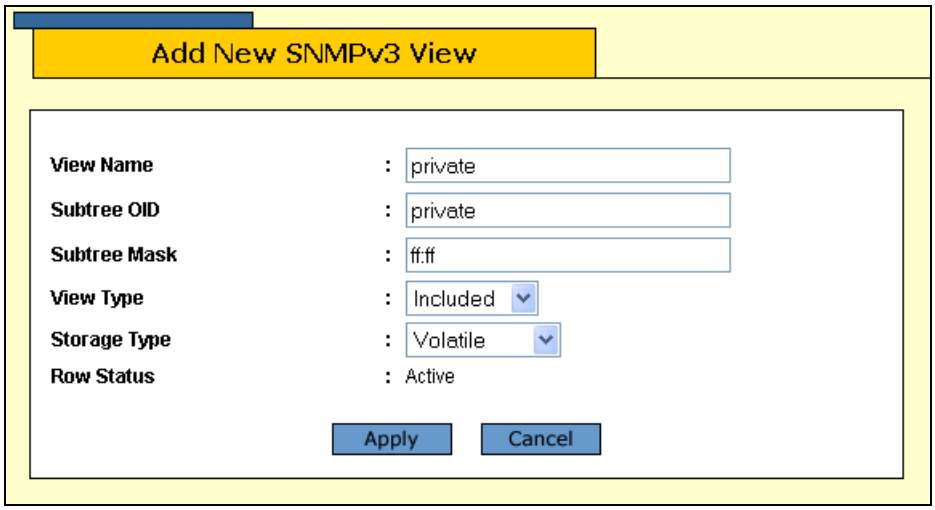

Figure 94. Add New SNMPv3 View Page

5. In the View Name field, enter a descriptive name for this view.

   Assign a name that reflects the subtree OID, for example, "internet." Enter a unique name of up to 32 alphanumeric characters.

Note
The “defaultViewAll” value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use the default value for an SNMPv3 View Table entry.

6. In the Subtree OID field, enter a subtree that this view will or will not be permitted to display.

   You can enter either a numeric value in hex format or the equivalent text name. For example, the OID hex format for TCP/IP is:

   ```
   1.3.6.1.2.1.6
   ```

   The text format is for TCP/IP is:

   ```
   tcp
   ```

7. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

   This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

   The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user’s view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

   ```
   1.3.6.1.2.1.2.2.1.0.3
   ```

   To restrict the user’s view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

   ```
   ff:bf
   ```

8. In the View Type field, enter one of the following view types:

   Included
   Enter this value to permit the user to see the subtree specified above.

   Excluded
   Enter this value to not permit the user to see the subtree specified above.

9. In the Storage Type field, enter a storage type for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the View Table. After making changes to a View Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile
Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 View Table.

11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a View Table Entry

To delete an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure**.

   The SNMPv3 View Table tab is shown in Figure 93 on page 245.

4. Click the button next to the View Table entry that you want to delete and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a View Table Entry

To modify an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to Configure View Table and then click **Configure** at the bottom of the tab.

   The SNMPv3 View Table tab is shown in Figure 93 on page 245.

4. Click the button next to the SNMPv3 View Table entry that you want to change and then click **Modify**.

   The Modify SNMPv3 View page is shown in Figure 95.

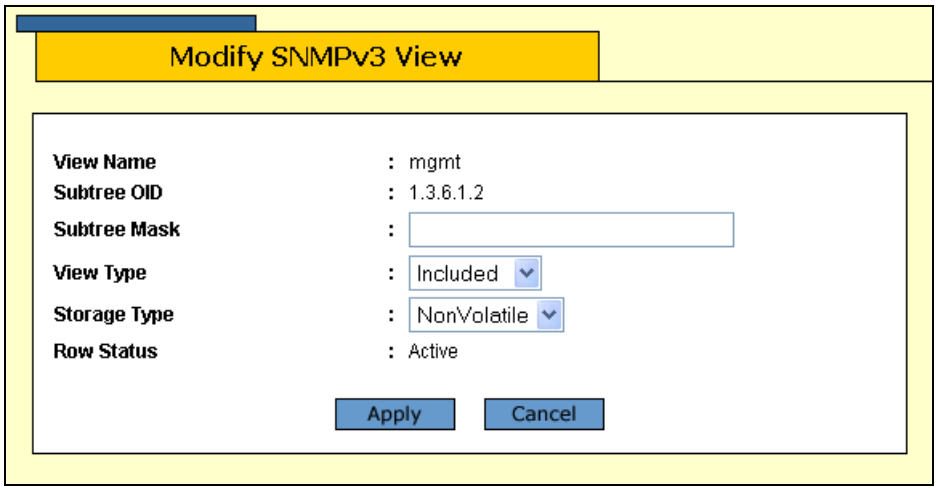

Figure 95. Modify SNMPv3 View Page

5. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

   This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

   The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user's view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

   ```
   1.3.6.1.2.1.2.2.1.0.3
   ```

   To restrict the user's view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

   ```
   ff:bf
   ```

6. In the View Type field, enter one of the following view types:

   Included
   Enter this value to permit the View Name to see the subtree specified above.

   Excluded
   Enter this value to not permit the View Name to see the subtree specified above.

7. In the Storage Type field, enter a storage type for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

8. Click **Apply**.

9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Access Table

You can create, delete, and modify an SNMPv3 Access Table entry. See the following procedures:

- “Creating an Access Table” on page 250
- “Deleting an Access Table Entry” on page 253
- “Modifying an Access Table Entry” on page 254

For information about the SNMPv3 Access Table, see Chapter 22, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating an Access Table

To create an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Access Table tab is shown in Figure 96.

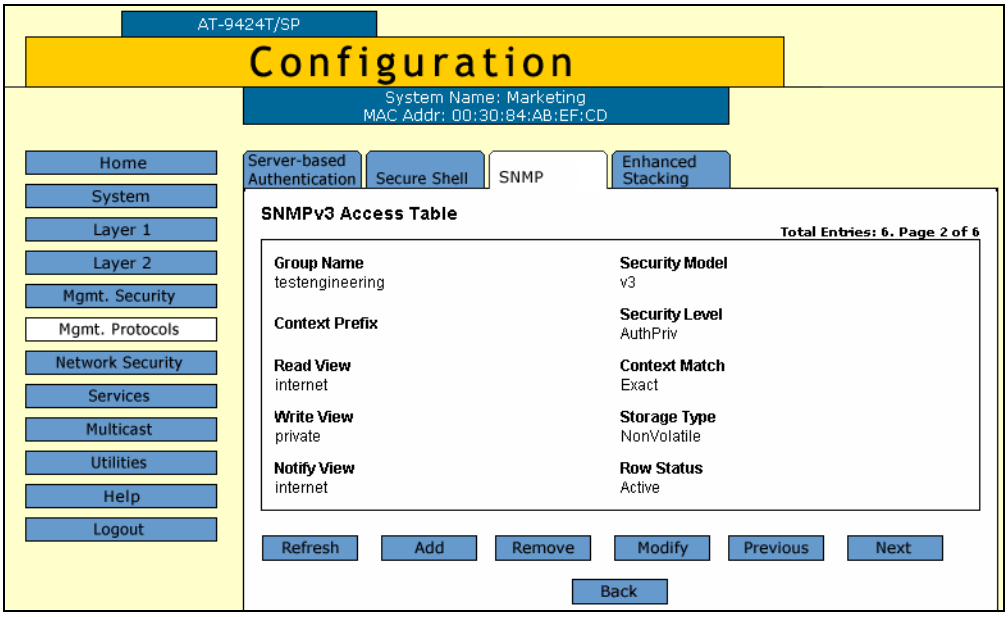

Figure 96. SNMPv3 Access Table Tab (Configuration)

4. To create an SNMPv3 Access Table entry, click **Add**.

   The Add New SNMPv3 Access page is shown in Figure 97.

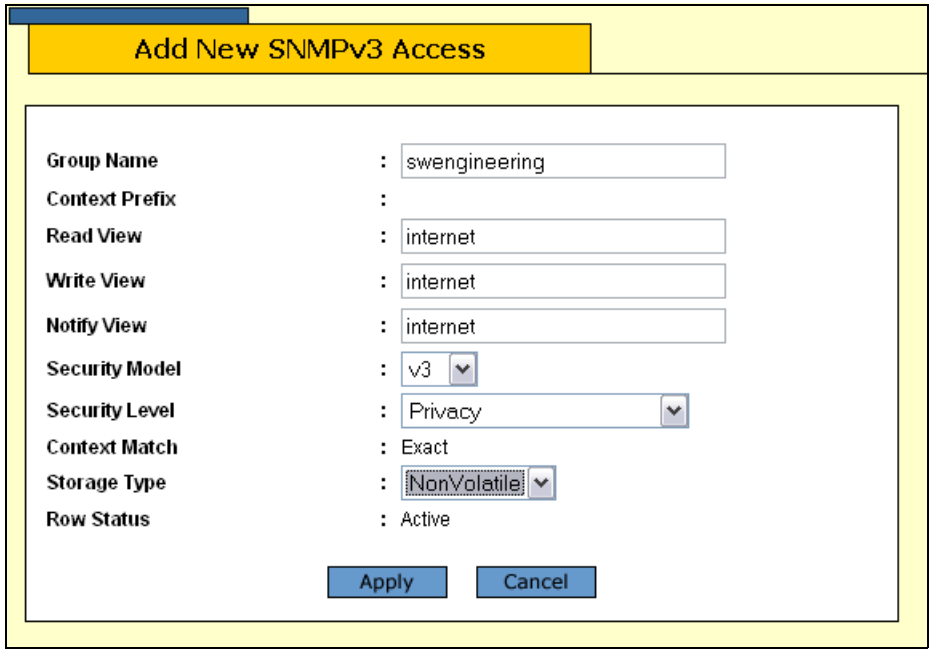

Figure 97. Add New SNMPv3 Access Page

5. In the Group Name field, enter a descriptive name of the group.

   The Group Name can consist of up to 32 alphanumeric characters.

   You are not required to enter a unique value here because the SNMPv3 Access Table entry is indexed with the Group Name, Security Model, and Security Level parameter values. However, a unique group name makes it easier for you to tell the groups apart.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   - defaultV1GroupReadOnly
   - defaultV1GroupReadWrite
   - defaultV2cGroupReadOnly
   - defaultV2cGroupReadWrite

   Note
   The Context Prefix field is a read only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

   This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

   This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

9. In the Security Model field, enter an SNMP protocol.

   Select one of the following SNMP protocols as the Security Model for this Group Name.

   v1
   Select this value to associate the Group Name with the SNMPv1 protocol.

   v2c
   Select this value to associate the Group Name with the SNMPv2c protocol.

   v3
   Select this value to associate the Group Name with the SNMPv3 protocol.

10. In the Security Level field, enter a security level.

    Select one of the following security levels:

    No Authentication/Privacy
    This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This option provides the least security.

    Note
    If you have selected SNMPv1 or SNMPv2c, N-NoAuthNoPriv is the only security level you can select.

    Authentication
    This option permits an authentication protocol, but not a privacy

protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy
This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Note
The Context Match field is a read only field. The Context Match field is always set to Exact.

11. In the Storage Type field, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

    Note
    The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

12. Click **Apply**.

13. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an Access Table Entry

To delete an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Access Table tab is shown in Figure 96 on page 250.

4. Click **Next** or **Previous** to display the Access Table entry that you want to delete.

5. Click **Remove**.

   A warning message is displayed. Click OK to remove the Access Table entry.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an Access Table Entry

To modify an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Access Table tab is shown in Figure 96 on page 250.

4. Click **Next** or **Previous** to display the Access Table entry that you want to change.

5. Click **Modify**.

   The Modify SNMPv3 Access page is shown in Figure 98.

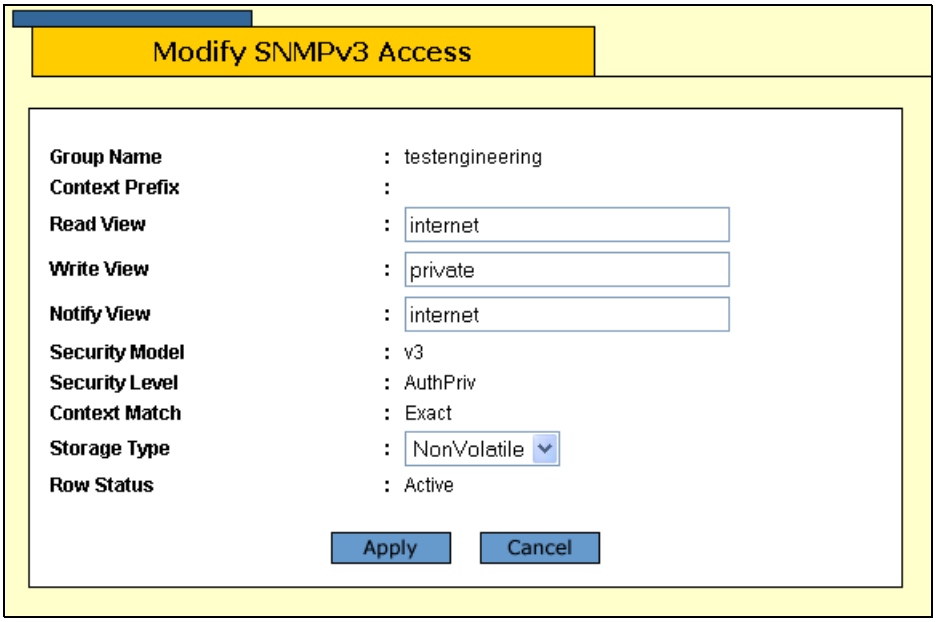

Figure 98. Modify SNMPv3 Access Page

Note
The Context Prefix field is a read-only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

Note
The Context Match field is a read only field. The Context Match field is always set to Exact.

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the Access Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Access Table.

11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 SecurityToGroup Table

You can create, delete, and modify an SNMPv3 SecurityToGroup Table entry. See the following procedures:

- "Creating a SecurityToGroup Table Entry" on page 257
- "Deleting a SecurityToGroup Table Entry" on page 260
- "Modifying a SecurityToGroup Table Entry" on page 260

For reference information about the SNMPv3 SecuritytoGroup Table, see Chapter 22, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a SecurityToGroup Table Entry

To create an entry in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 99.

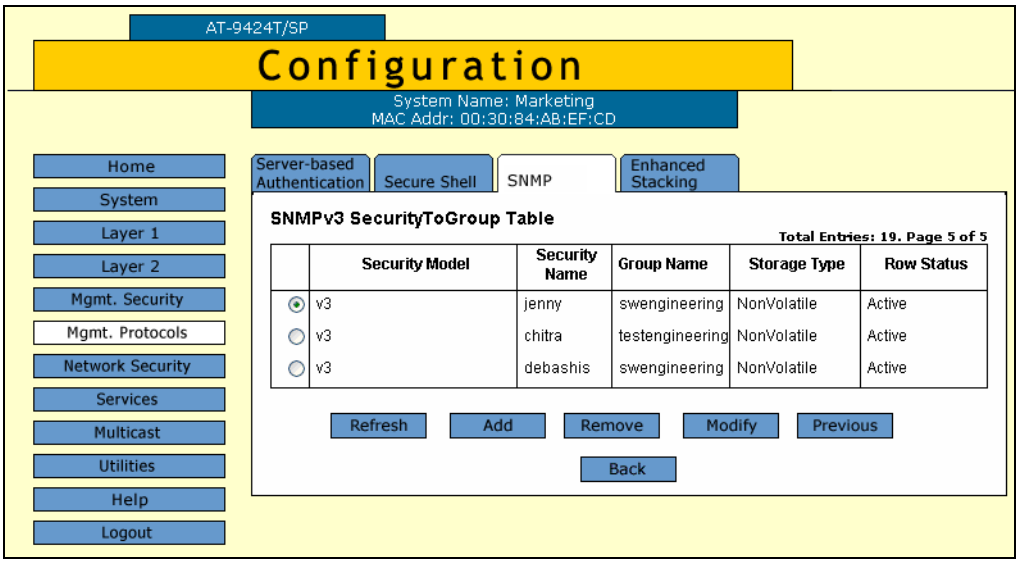

Figure 99. SNMPv3 SecurityToGroup Table Tab (Configuration)

4. To create an SNMPv3 SecurityToGroup Table entry, click **Add**.

   The Add New SNMPv3 SecurityToGroup page is shown in Figure 100.

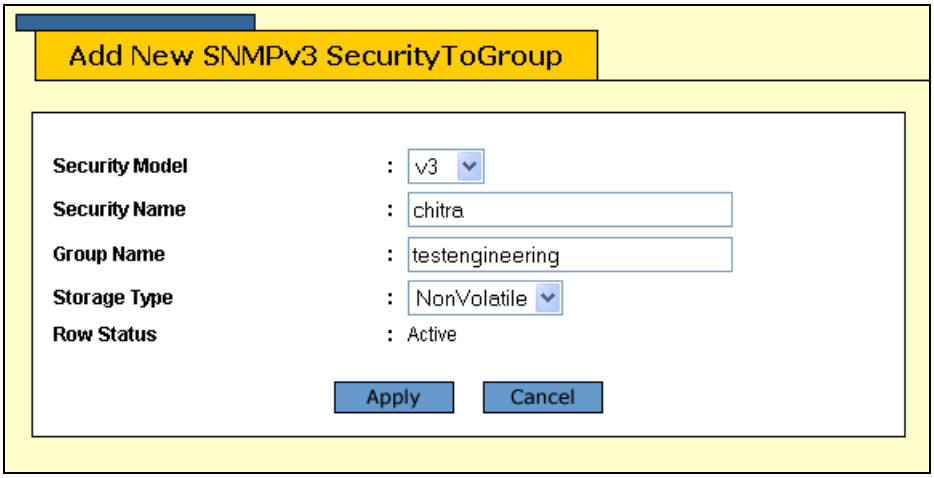

Figure 100. Add New SNMPv3 SecurityToGroup Page

5. In the Security Model field, select the SNMP protocol that was configured for this User Name.

   Choose from the following:

   v1
   Select this value to associate the Group Name with the SNMPv1 protocol.

v2c
Select this value to associate the Group Name with the SNMPv2c protocol.

v3
Select this value to associate the Group Name with the SNMPv3 protocol.

6. In the Security Name field, enter the User Name that you want to associate with a group.

   Enter a User Name that you configured in "Creating a User Table Entry" on page 236.

7. In the Group Name field, enter a Group Name that you configured in the Access Table.

   See "Creating an Access Table" on page 250.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   - defaultV1GroupReadOnly
   - defaultV1GroupReadWrite
   - defaultV2cGroupReadOnly
   - defaultV2cGroupReadWrite

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

9. Click **Apply**.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a SecurityToGroup Table Entry

To delete an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table**, and then click **Configure** at the bottom of the tab.

   The SNMPv3 SecurityToGroup Table tab is shown in Figure 99 on page 258.

4. Click the button next to the SecurityToGroup Table entry that you want to delete and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a SecurityToGroup Table Entry

To modify an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 SecurityToGroup Table tab is shown in Figure 99 on page 258.

4. Click the button next to the SecurityToGroup Table entry that you want to change, and then click **Modify**.

   The Modify SNMPv3 SecurityToGroup page is shown in Figure 101.

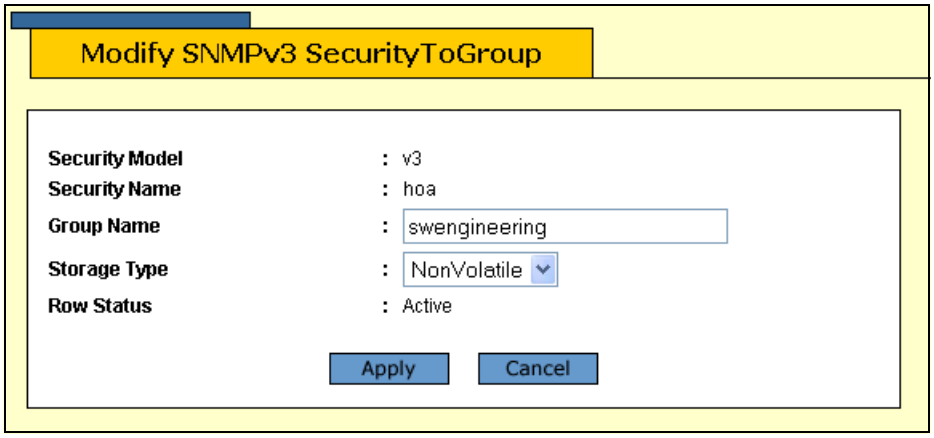

Figure 101. Modify SNMPv3 SecurityToGroup Page

5. In the Group Name field, enter a Group Name that you configured in the SNMPv3 Access Table.

   See "Creating an Access Table" on page 250.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   - defaultV1GroupReadOnly
   - defaultV1GroupReadWrite
   - defaultV2cGroupReadOnly
   - defaultV2cGroupReadWrite

6. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

7. Click **Apply** to update the SNMPv3 SecurityToGroup Table.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Notify Table

You can create, delete, and modify an SNMPv3 Notify Table entry. See the following procedures:

- "Creating a Notify Table Entry" on page 263
- "Deleting a Notify Table Entry" on page 265
- "Modifying a Notify Table Entry" on page 266

For reference information about the SNMPv3 Notify Table, see Chapter 22, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Notify Table Entry

To create an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 102.

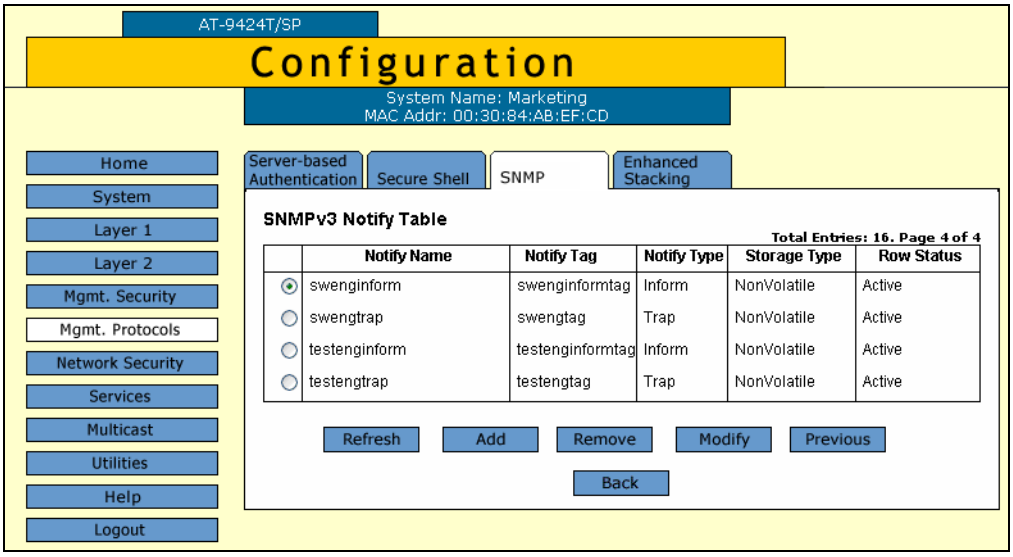

Figure 102. SNMPv3 Notify Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Notify page is shown in Figure 103.

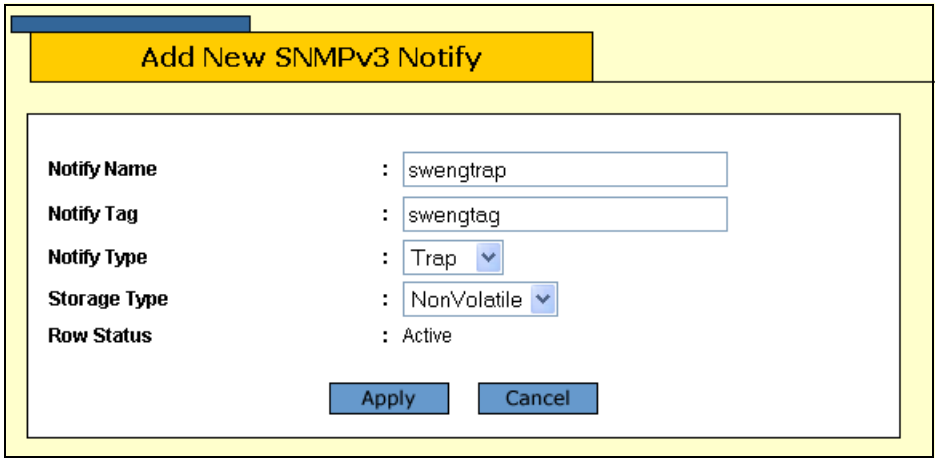

Figure 103. Add New SNMPv3 Notify Page

5. In the Notify Name field, enter the name associated with this trap message.

   Enter a descriptive name of up to 32 alphanumeric characters. For example, you might want to define a trap message for hardware engineering and enter a value of “hardwareengineeringtrap” for the Notify Name.

6. In the Notify Tag field, enter a description name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters.

7. In the Notify Type field, enter one of the following message types:

   Trap
   Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the host.

   Inform
   Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a NonVolatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Notify Table.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Notify Table Entry

To delete an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 102 on page 264.

4. Click the button next to the Notify Table entry that you want to delete, and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Notify Table Entry

To modify an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to Configure Notify Table, and then click **Configure** at the bottom of the tab.

   The SNMPv3 Notify Table tab is shown in Figure 102 on page 264.

4. Click the button next to the table entry that you want to change and then click **Modify**.

   The Modify SNMPv3 Notify page is shown in Figure 104.

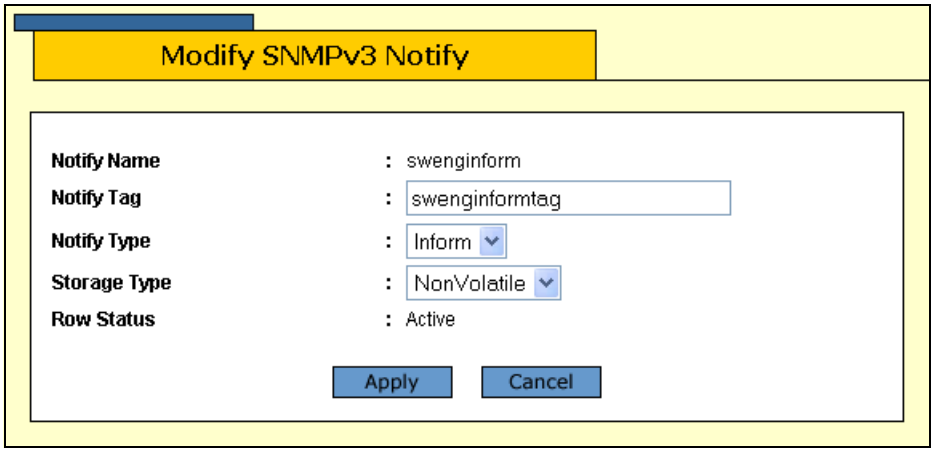

Figure 104. Modify SNMPv3 Notify Page

5. In the Notify Tag field, enter a description name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters.

6. In the Notify Type field, enter one of the following message types:

   Trap
   Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the host.

   Inform
   Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

7. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a NonVolatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 Notify Table.

9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Target Address Table

You can create, delete, and modify an SNMPv3 Target Address Table entry. See the following procedures:

- “Creating a Target Address Table Entry” on page 268
- “Deleting a Target Address Table Entry” on page 271
- “Modifying Target Address Table Entry” on page 272

For reference information about the SNMPv3 Target Address Table, see Chapter 22, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a Target Address Table Entry

To create an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 105.

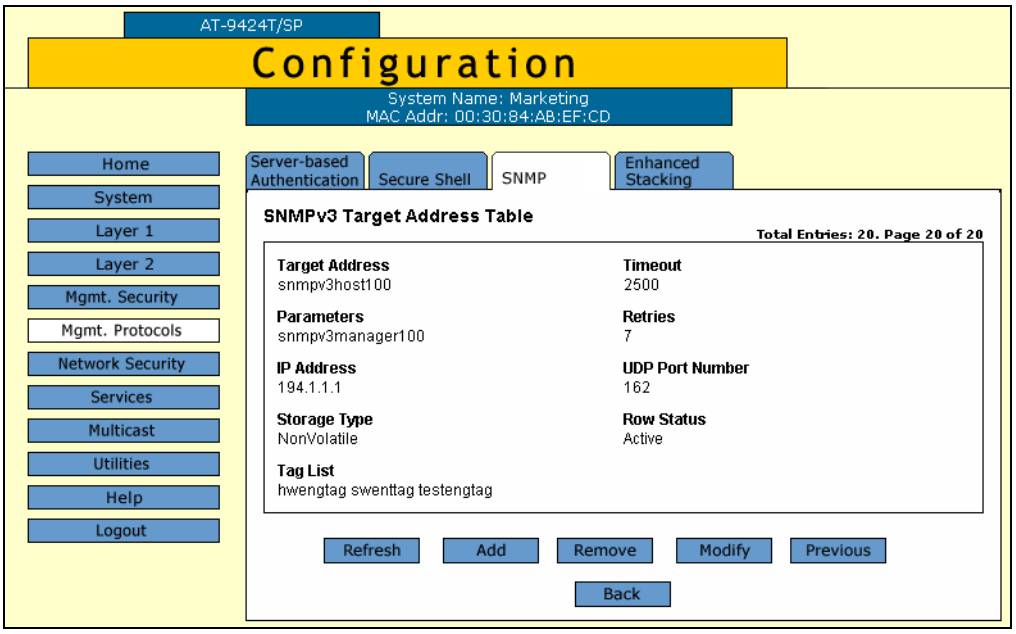

Figure 105. SNMPv3 Target Address Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Target Address page is shown in Figure 106.

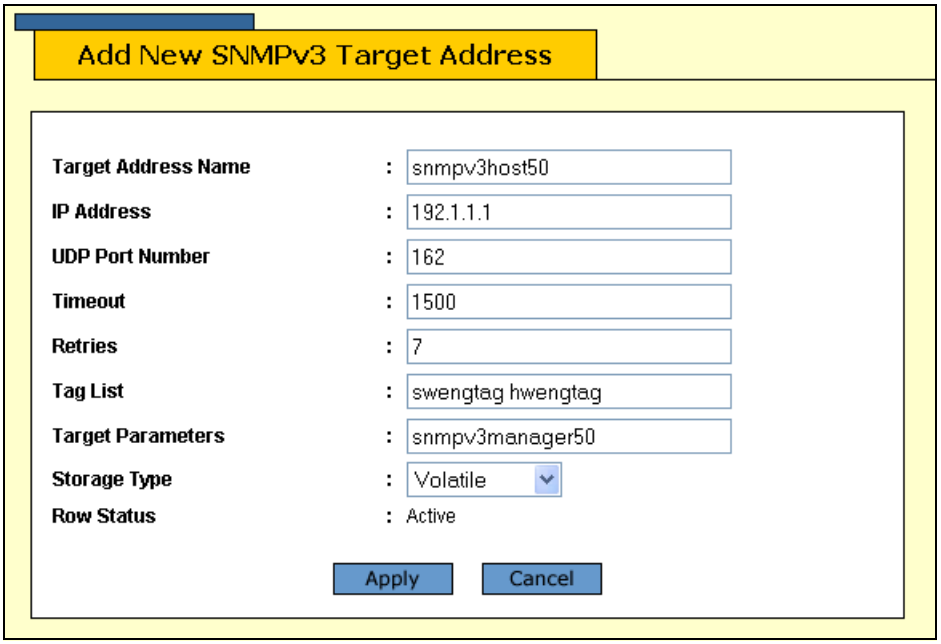

Figure 106. Add New SNMPv3 Target Address Page

5. In the Target Address Name field, enter the name of the SNMP manager, or host, that manages the SNMP activity on your switch.

You can enter a name of up to 32 alphanumeric characters.

6. In the IP Address field, enter the IP address of the host.

   Use the following format for an IP address:
   XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

   You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

   When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

   When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured in a SNMPv3 Notify Table with the Notify Tag parameter.

    See “Creating a Notify Table Entry” on page 263. Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries, for example:

    ```
    hwengtag swengtag testengtag
    ```

11. In the Target Parameters field, enter a Target Parameters name.

    This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the SNMPv3 Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile
Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Address Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Target Address Table Entry

To delete an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Address Table tab is shown in Figure 105 on page 269.

4. Click **Next** or **Previous** to display the SNMPv3 Target Address Table entry that you want to delete.
5. Click **Remove**.

   A warning message is displayed.

6. Click **OK**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying Target Address Table Entry

To modify an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Address Table tab is shown in Figure 105 on page 269.

4. Click **Next** or **Previous** to display the Target Address Table entry that you want to change.

5. Click **Modify**.

   The Modify SNMPv3 Target Address page is shown Figure 107.

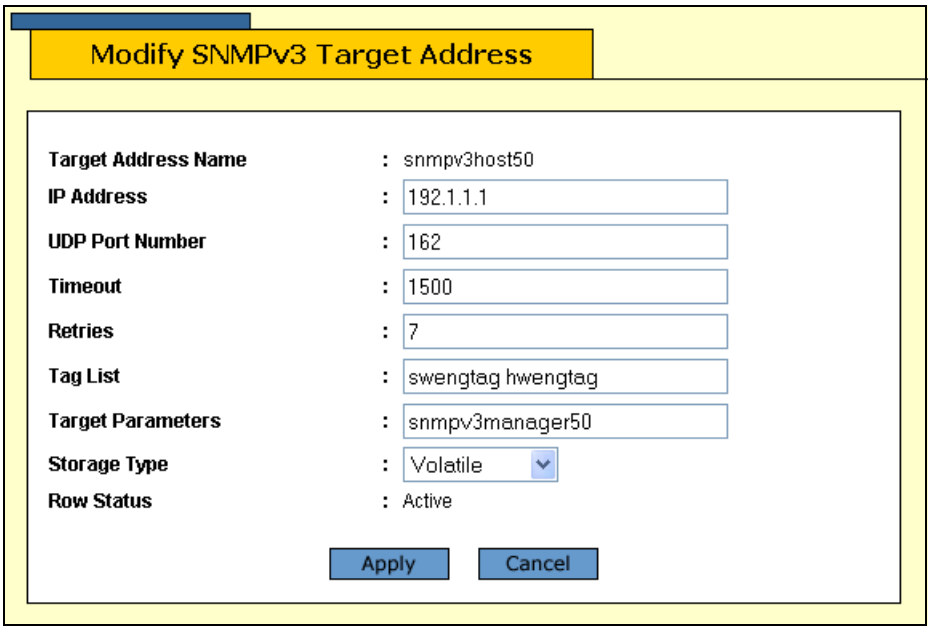

Figure 107. Modify SNMPv3 Target Address Page

6. In the IP Address field, enter the IP address of the host.

   Use the following format for an IP address:
   XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

   You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

   When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

   When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured with the Notify Tag parameter in a Notify Table entry.

    See "Creating a Notify Table Entry" on page 263. Enter a Tag List of up to 256-alphanumeric characters. Use a space to separate entries, for example:

    ```
    hwengtag swengtag testengtag
    ```

11. In the Target Parameters field, enter a Target Parameters name.

    This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to an Target Address Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

13. Click **Apply** to update the SNMPv3 Target Address Table.

14. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Target Parameters Table

You can create, delete, and modify an SNMPv3 Target Parameters Table entry. See the following procedures:

- "Creating a Target Address Table Entry" on page 268
- "Deleting a Target Address Table Entry" on page 271
- "Modifying Target Address Table Entry" on page 272

For reference information about the SNMPv3 Target Parameters Table, see Chapter 22, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Target Parameters Table Entry

To create an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Parameters Table tab is shown in Figure 108.

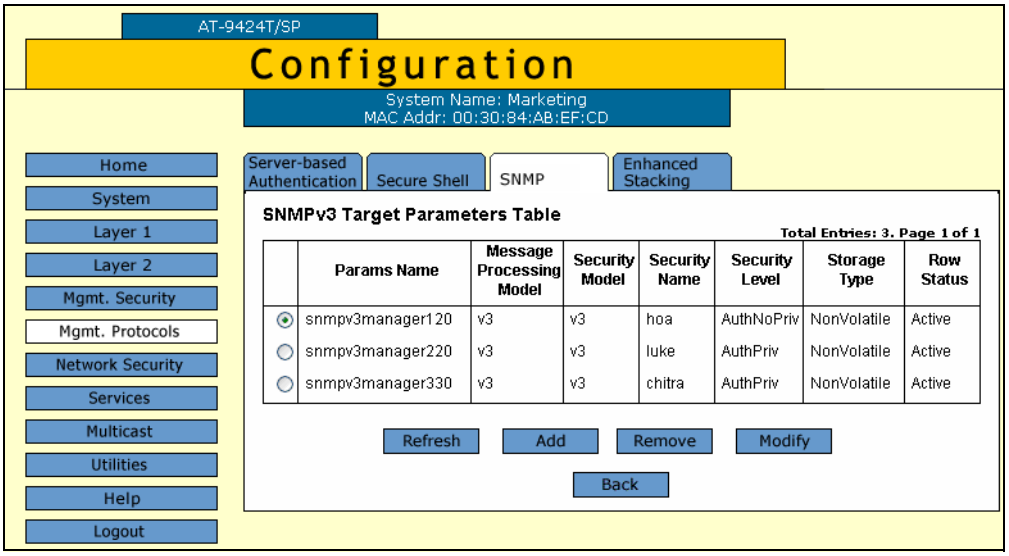

Figure 108. SNMPv3 Target Parameters Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Target Parameter page is shown in Figure 109.

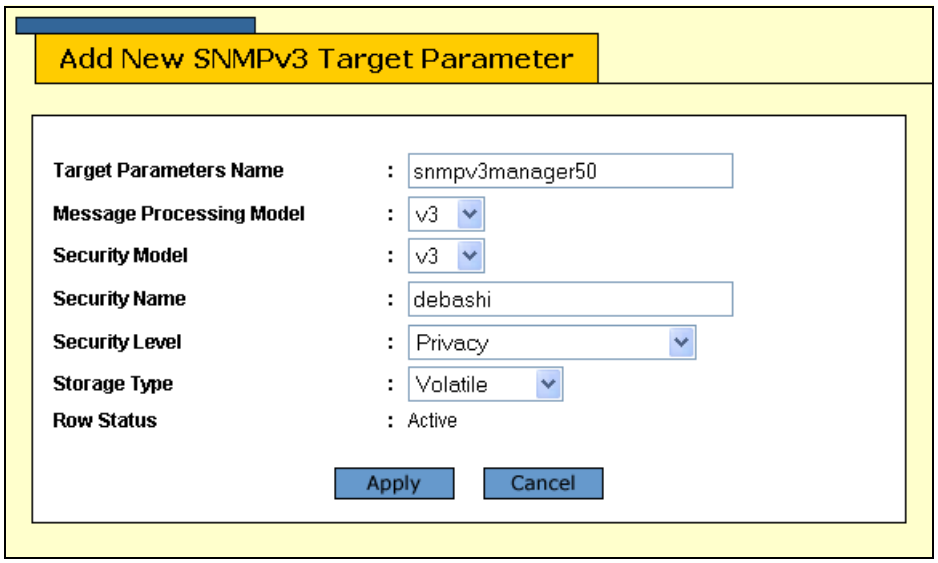

Figure 109. Add New SNMPv3 Target Parameters Page

5. In the Target Parameters Name field, enter a name of the SNMP manager or host.

   Enter a value of up to 32 alphanumeric characters.

   Note
   Enter a value for the Message Processing Model parameter only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the Message Processing Model is automatically assigned to SNMPv3.

6. In the Message Processing Model field, enter a Security Model that is used to process messages.

   Select one of the following SNMP protocols:

   v1
   Select this value to process messages with the SNMPv1 protocol.

   v2c
   Select this value to process messages with the SNMPv2c protocol.

   v3
   Select this value to process messages with the SNMPv3 protocol.

7. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

v1
Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

v2c
Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

v3
Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

8. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

   See "Creating a User Table Entry" on page 236.

9. In the Security Level field, select one of the following Security Levels:

   Note
   The value you configure for the Security Level must match the value configured for the User Name in the User Table Menu. See "Creating a User Table Entry" on page 236.

   No Authentication/Privacy
   This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

   Note
   If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

   Authentication
   This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

   Privacy
   This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

10. In the Storage Type parameter, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

    Note
    The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 Target Parameters Table.

12. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Target Parameters Table Entry

To delete an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Parameters Table tab is shown in Figure 108 on page 275.

4. Click the button next to the Target Parameters Table entry that you want to delete and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Target Parameters Table Entry

To modify an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Parameters Table tab is shown in Figure 108 on page 275.

4. Click the button next to the Target Parameters Table entry that you want to change, and then click **Modify**.

   The Modify SNMPv3 Target Parameter page is shown in Figure 110 on page 279.

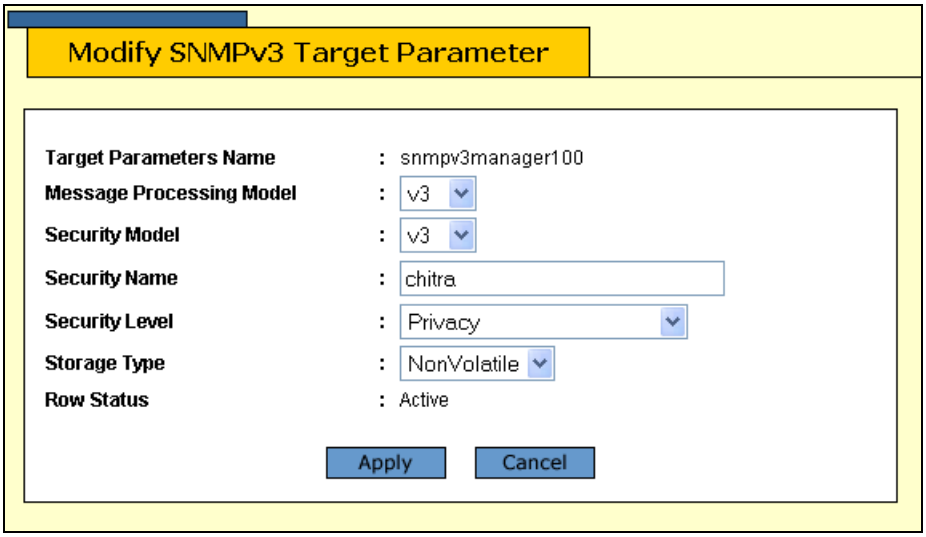

Figure 110. Modify SNMPv3 Target Parameter Page

Note
Enter a value for the Message Processing Model field only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the switch automatically assigns the Message Processing Model to SNMPv3.

5. In the Message Processing Model field, enter a Security Model that is used to process messages.

   Select one of the following SNMP protocols:

   v1
   Select this value to process messages with the SNMPv1 protocol.

   v2c
   Select this value to process messages with the SNMPv2c protocol.

   v3
   Select this value to process messages with the SNMPv3 protocol.

6. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

   v1
   Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

   v2c
   Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

   v3
   Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

7. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

   See “Creating a User Table Entry” on page 236.

8. In the Security Level field, select one of the following Security Levels:

   Note
   The value you configure for the Security Level must match the value configured for the User Name in the SNMPv3 User Table Menu. See “Creating a User Table Entry” on page 236.

   No Authentication/Privacy
   This option represents neither an authentication nor privacy protocol.

Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note
If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication
This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy
This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

9. In the Storage Type parameter, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry will take effect immediately.

10. Click **Apply** to update the SNMPv3 Target Parameters Table.

11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Community Table

You can create, delete, and modify an SNMPv3 Community Table entry. See the following procedures:

- “Creating an SNMPv3 Community Table Entry” on page 282
- “Deleting an SNMPv3 Community Table Entry” on page 285
- “Modifying an SNMPv3 Community Table Entry” on page 285

For reference information about the SNMPv3 Community Table, see Chapter 22, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Note
Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

Creating an SNMPv3 Community Table Entry

To create an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 111.

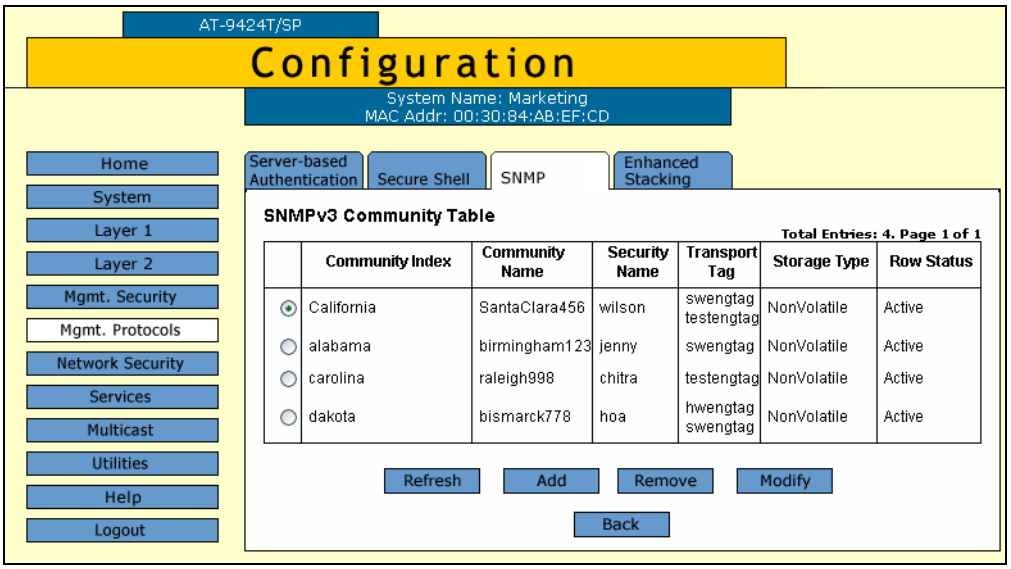

Figure 111. SNMPv3 Community Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Community page is shown in Figure 112.

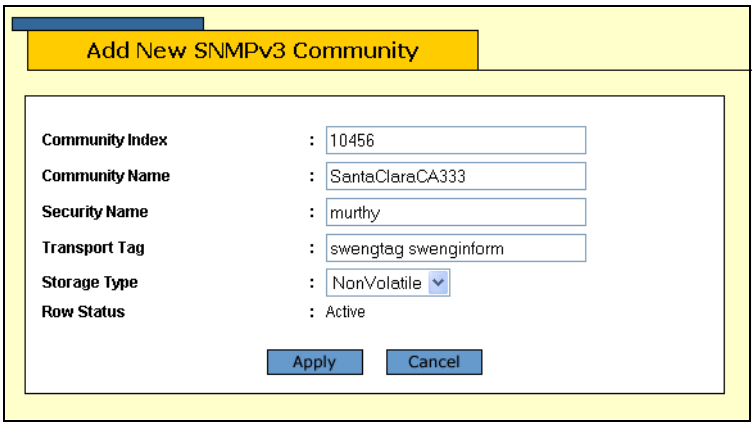

Figure 112. Add New SNMPv3 Community Page

5. In the Community Index field, enter a numerical value for this Community.

   This parameter is used to index the other parameters in an SNMPv3 Community Table entry. Enter a value of up to 32- alphanumeric characters.

6. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

Note
Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

7. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

   This name must be unique. Enter a value of up to 32 alphanumeric characters.

   Note
   Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

8. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

   The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See “Creating a Target Address Table Entry” on page 268.

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

10. Click **Apply**.
11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an SNMPv3 Community Table Entry

To delete an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Community Table tab is shown in Figure 111 on page 283.

4. Click the button next to the SNMPv3 Community Table entry that you want to delete and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an SNMPv3 Community Table Entry

To modify an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 89 on page 234.

3. In the SNMPv3 section, click the button next to **Configure Community Table**, and then click **Configure** at the bottom of the tab.

   The SNMPv3 Community Table tab is shown in Figure 111 on page 283.

4. Click the button next to the SNMPv3 Community Table entry that you want to change and then click **Modify**.

   The Modify SNMPv3 Community page is shown in Figure 113.

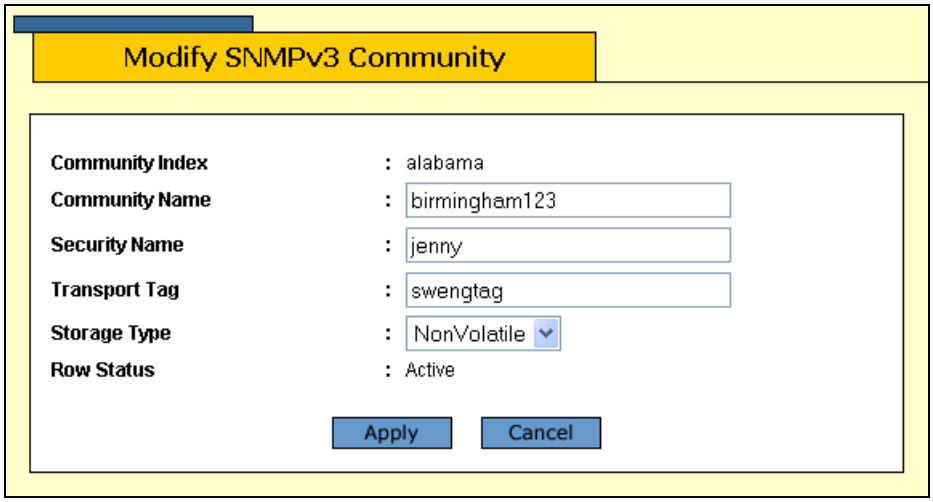

Figure 113. Modify SNMPv3 Community Page

5. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

   The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

   Note
   Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

6. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

   This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note
Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

7. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

   The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See "Creating a Target Address Table Entry" on page 268.

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Community Table.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying SNMPv3 Tables

This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

- ❒ “Displaying User Table Entries,” next
- ❒ “Displaying View Table Entries” on page 290
- ❒ “Displaying Access Table Entries” on page 291
- ❒ “Displaying SecurityToGroup Table Entries” on page 292
- ❒ “Displaying Notify Table Entries” on page 293
- ❒ “Displaying Target Address Table Entries” on page 294
- ❒ “Displaying Target Parameters Table Entries” on page 295
- ❒ “Displaying SNMPv3 Community Table Entries” on page 296

Displaying User Table Entries

To display entries in the SNMPv3 User Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Mgmt. Protocols**.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab displayed by default, as shown in Figure 13 on page 62.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 114.

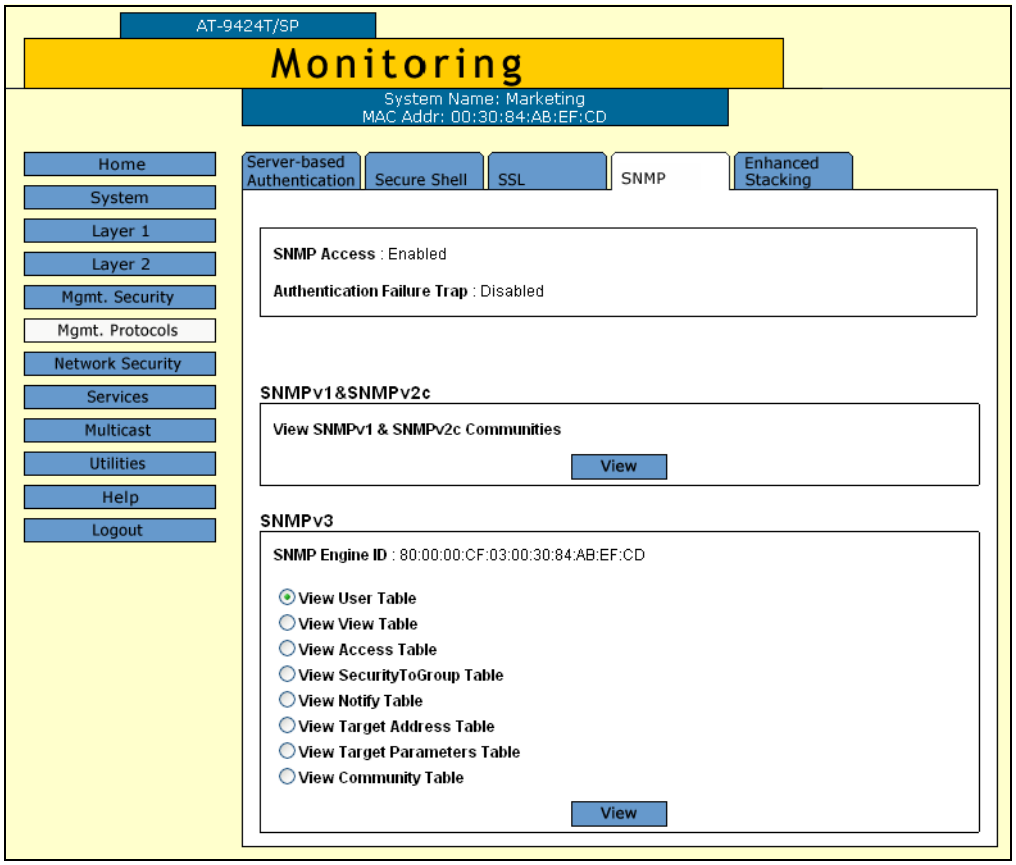

Figure 114. SNMP Tab (Monitoring)

4. In the SNMPv3 section, click the button next to View User Table and then click **View** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 115.

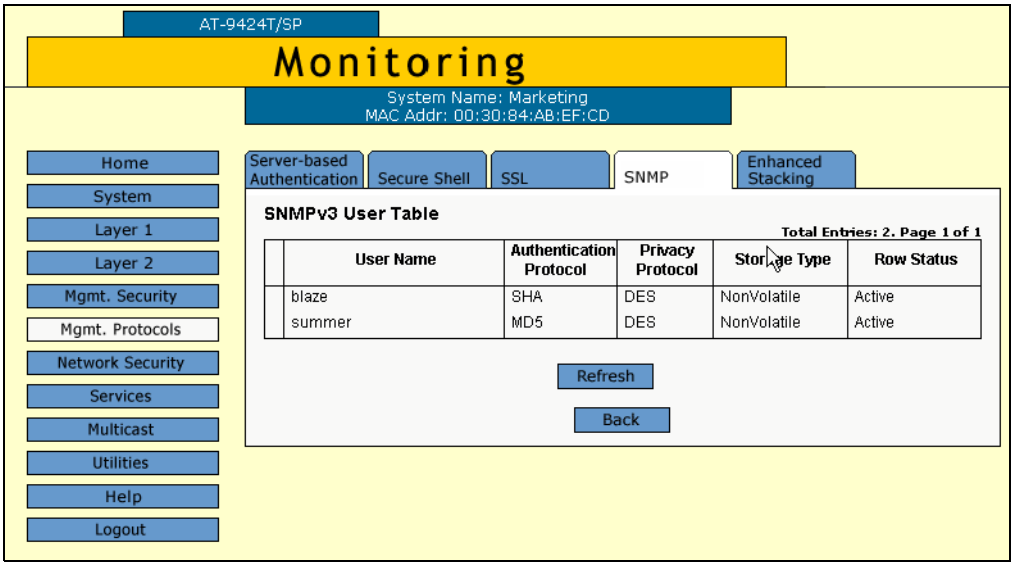

Figure 115. SNMPv3 User Table Tab (Monitoring)

Displaying View Table Entries

To display entries in the SNMPv3 View Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, click the button next to **View View Table** and then click **View** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 116.

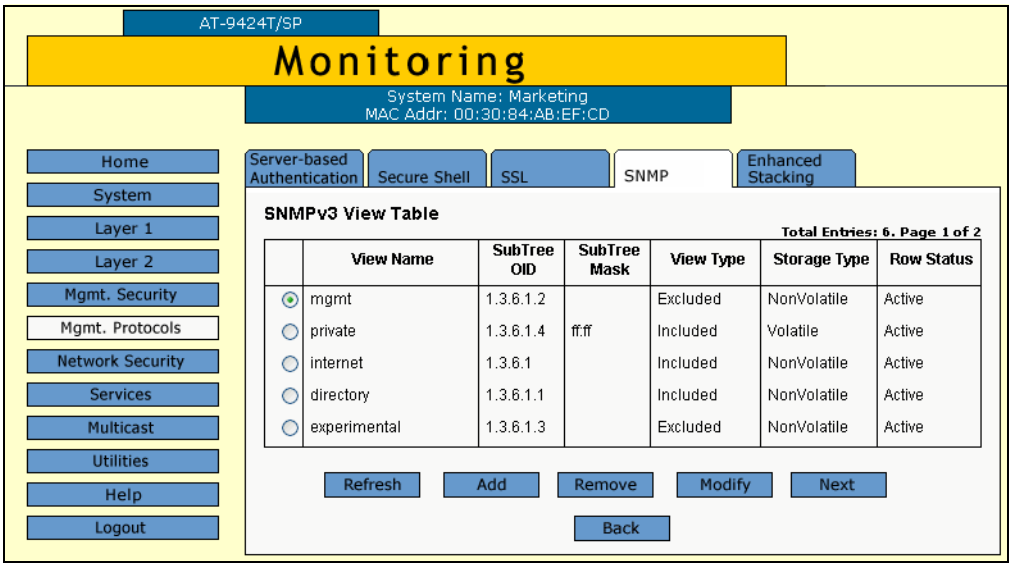

Figure 116. SNMPv3 View Table Tab (Monitoring)

Displaying Access Table Entries

To display entries in the SNMPv3 Access Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, click the button next to **View Access Table** and then click **View** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 117.

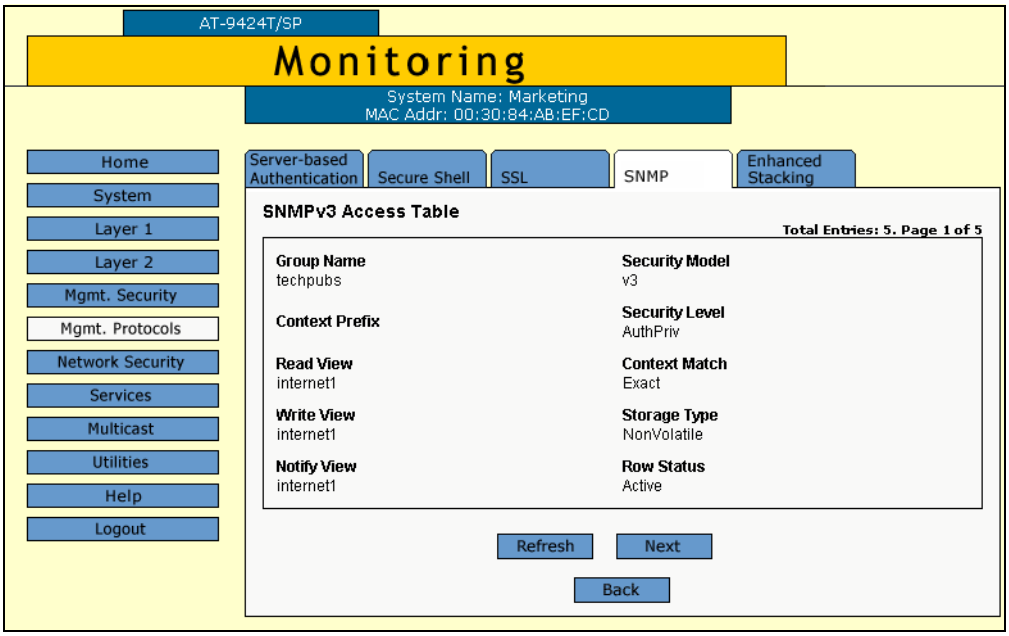

Figure 117. SNMPv3 Access Table Tab (Monitoring)

Displaying SecurityToGroup Table Entries

To display entries in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, click the button next to the **View SecurityToGroup Table** and then click **View** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 118.

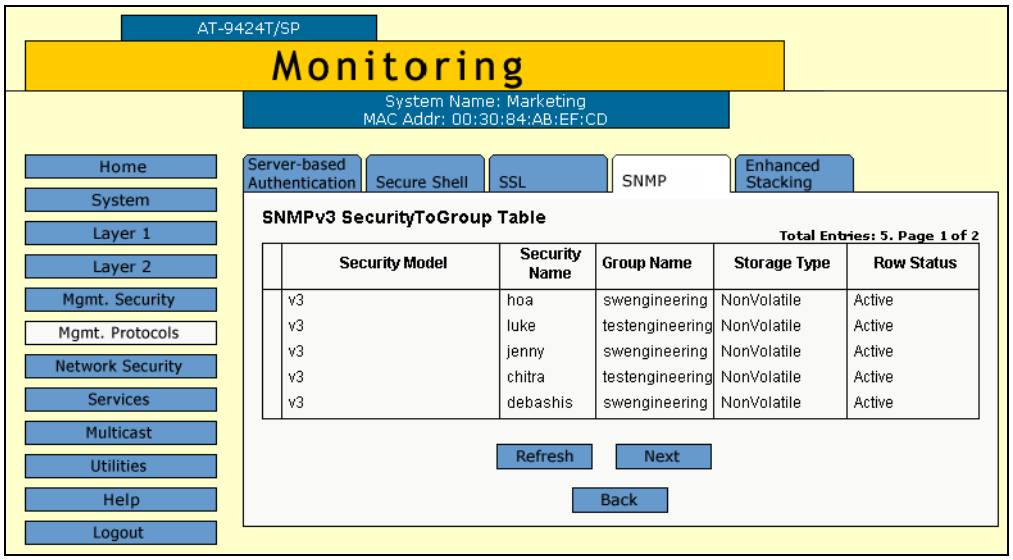

Figure 118. SNMPv3 SecurityToGroup Table Tab (Monitoring)

Displaying Notify Table Entries

To display entries in the SNMPv3 Notify Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, click the button next to **View Notify Table** and then click **View** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 119.

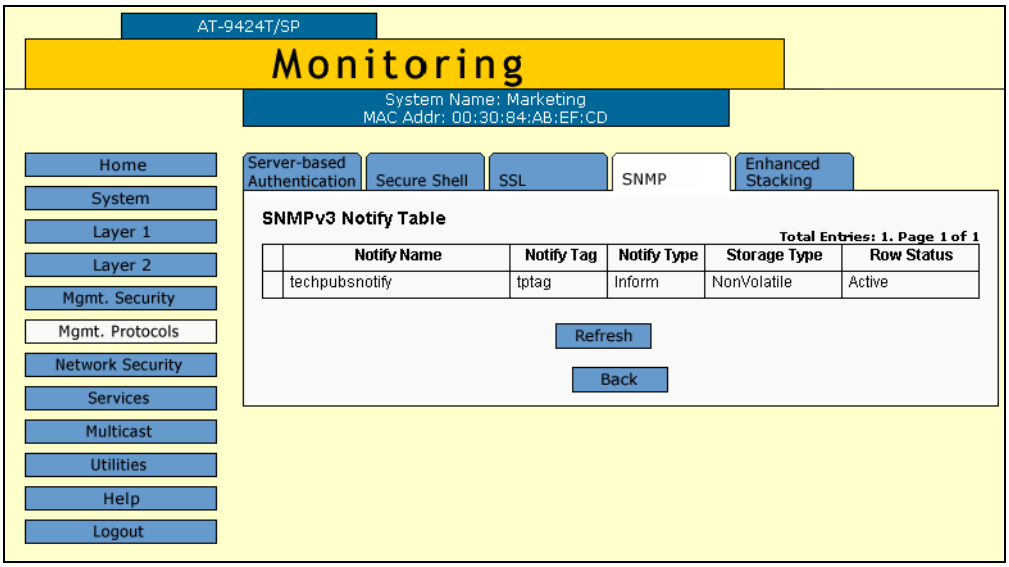

Figure 119. SNMPv3 Notify Table Tab (Monitoring)

Displaying Target Address Table Entries

To display entries in the SNMPv3 Target Address Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** Tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, lick the button next to **View Target Address Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 120.

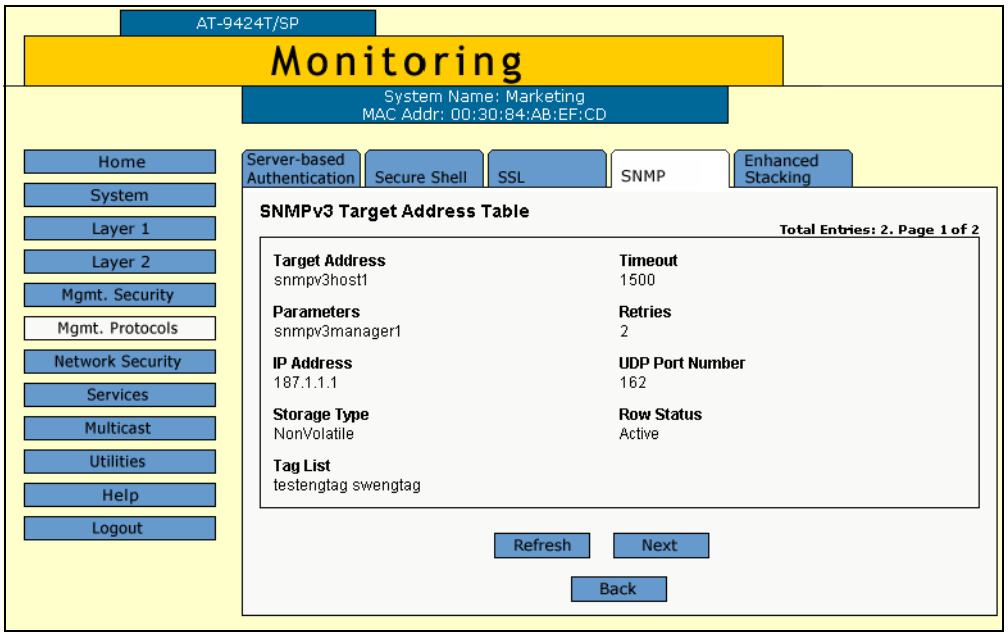

Figure 120. SNMPv3 Target Address Table Tab (Monitoring)

Displaying Target Parameters Table Entries

To display entries in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, click the button next to the **View Target Parameters Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 121.

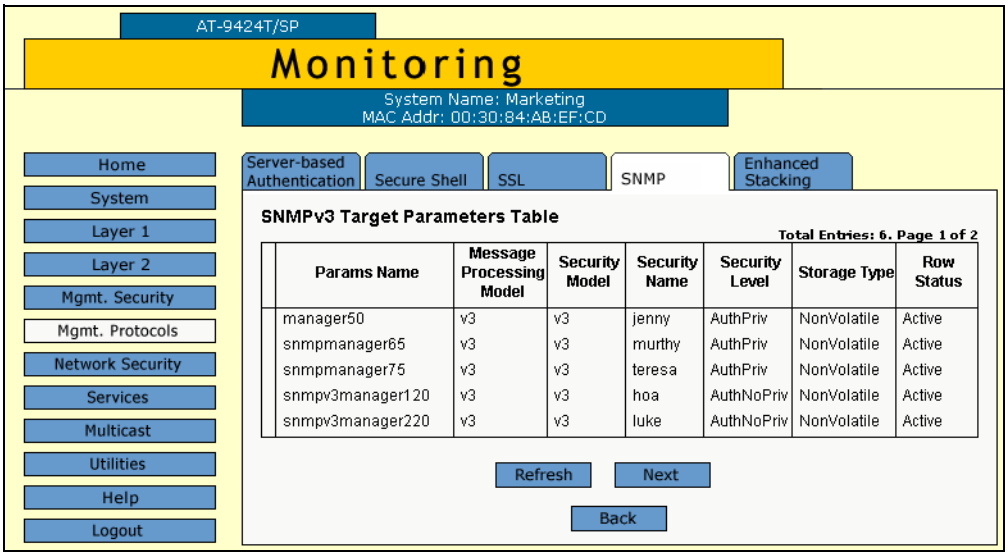
AT-9424T/SP
Monitoring
System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD
Home
System
Layer 1
Layer 2
Mgmt. Security
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Help
Logout
Server-based Authentication
Secure Shell
SSL
SNMP
Enhanced Stacking
SNMPv3 Target Parameters Table
Total Entries: 6. Page 1 of 2
Params Name | Message Processing Model | Security Model | Security Name | Security Level | Storage Type | Row Status
manager50 | v3 | v3 | jenny | AuthPriv | NonVolatile | Active
snmpmanager65 | v3 | v3 | murthy | AuthPriv | NonVolatile | Active
snmpmanager75 | v3 | v3 | teresa | AuthPriv | NonVolatile | Active
snmpv3manager120 | v3 | v3 | hoa | AuthNoPriv | NonVolatile | Active
snmpv3manager220 | v3 | v3 | luke | AuthNoPriv | NonVolatile | Active
Refresh
Next
Back

Figure 121. SNMPv3 Target Parameters Table Tab (Monitoring)

Displaying SNMPv3 Community Table Entries

To display entries in the SNMPv3 Community Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 114 on page 289.

3. In the SNMPv3 section, click the button next to **View Community Table** and then click **View** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 122.

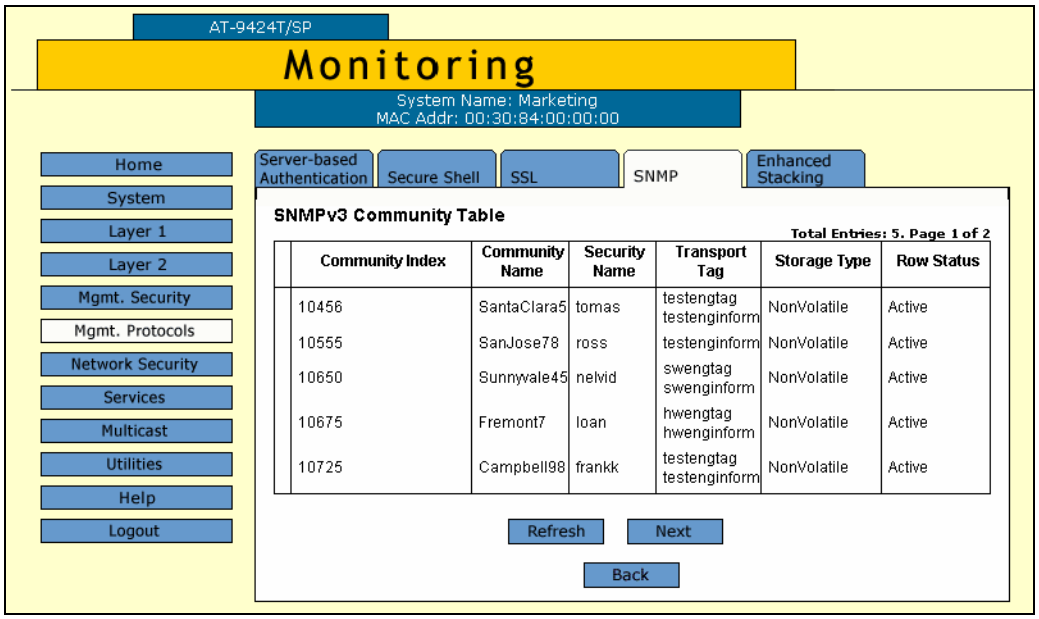

Figure 122. SNMPv3 Community Table Tab (Monitoring)

Section IV

Spanning Tree Protocols

The chapters in this section contain the procedures for configuring the spanning tree protocols. The chapters include:

- Chapter 19, “Spanning Tree and Rapid Spanning Tree Protocols” on page 301
- Chapter 20, “Multiple Spanning Tree Protocol” on page 319

Chapter 19

Spanning Tree and Rapid Spanning Tree Protocols

This chapter explains how to configure the STP and RSTP parameters on an AT-9400 Series switch. The sections in the chapter include:

- ❒ “Enabling or Disabling a Spanning Tree Protocol” on page 302
- ❒ “Configuring STP” on page 304
- ❒ “Configuring RSTP” on page 312

Note
For background information on spanning tree, refer to Chapter 23, “Spanning Tree and Rapid Spanning Tree Protocols,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Multiple Spanning Tree Protocol (MSTP) is described in Chapter 20, “Multiple Spanning Tree Protocol” on page 319.

Enabling or Disabling a Spanning Tree Protocol

To enable or disable spanning tree on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 123.

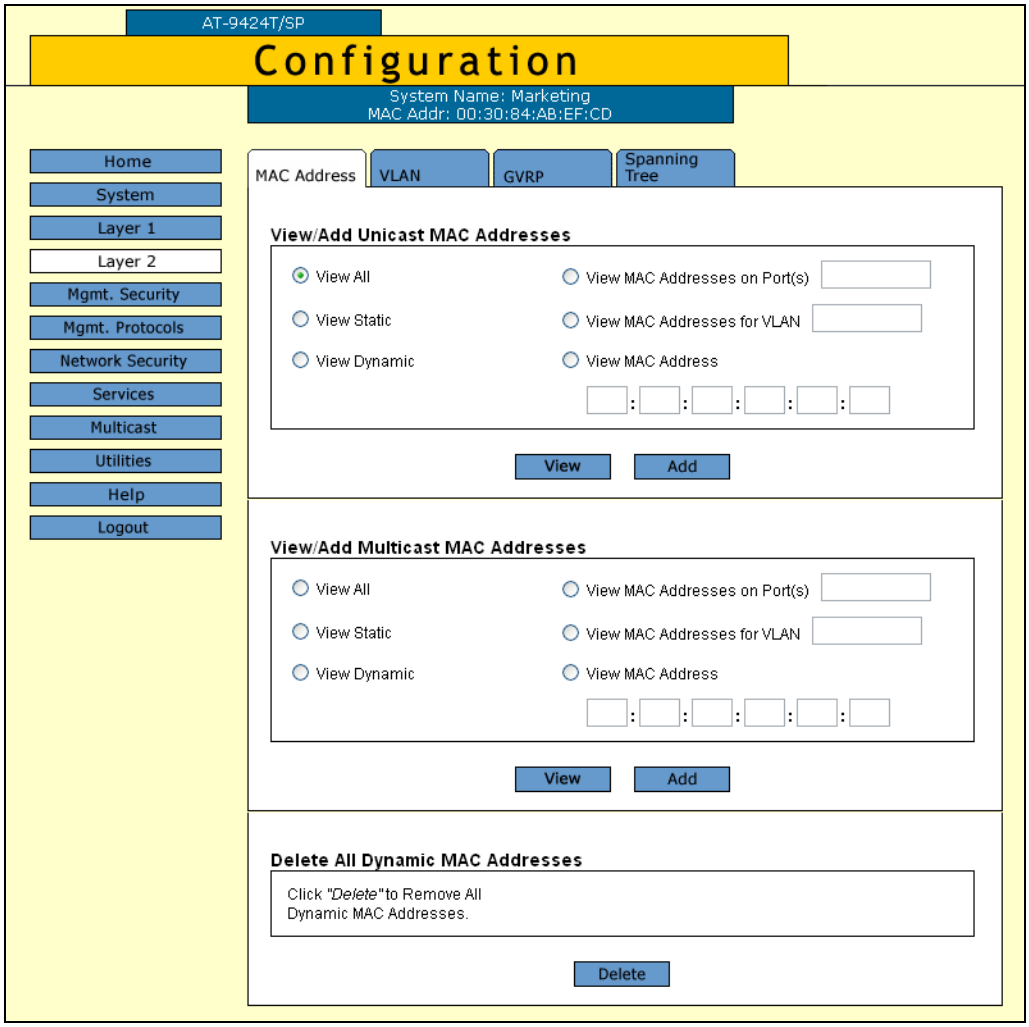

Figure 123. MAC Address Tab (Configuration)

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 124.

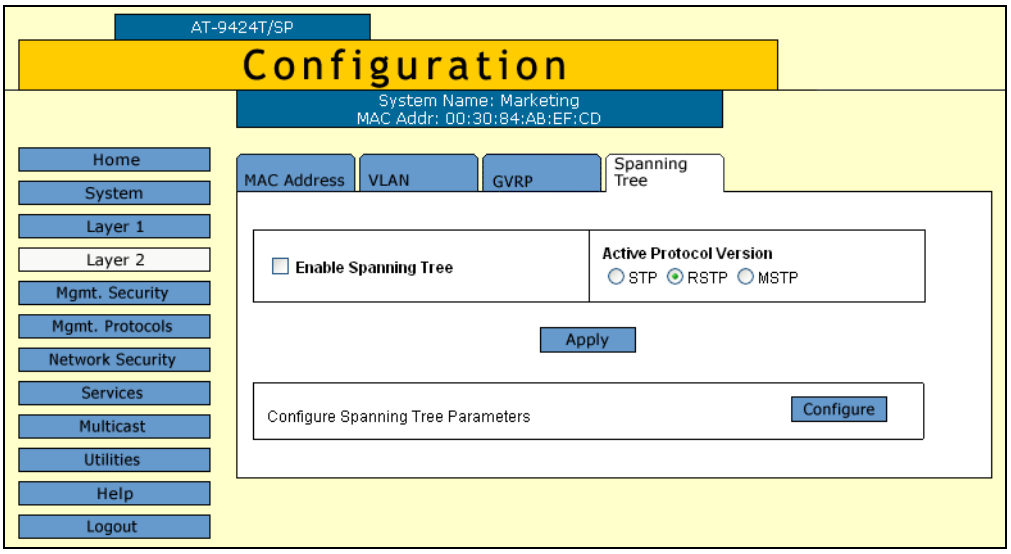

Figure 124. Spanning Tree Tab (Configuration)

4. To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.

5. To select a spanning tree version, for the Active Protocol Version parameter click **STP**, **RSTP**, or **MSTP**. The default is RSTP.

   Note
   Only one spanning tree protocol can be active on the switch at a time.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

8. If you activated STP, go to "Configuring STP" on page 304. If you activated RSTP go to Step "Configuring RSTP" on page 312. If you activated MSTP, go to Chapter 20, "Multiple Spanning Tree Protocol" on page 319.

Configuring STP

Caution
The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

To configure STP, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

The Configure STP Parameters tab is shown in Figure 125.

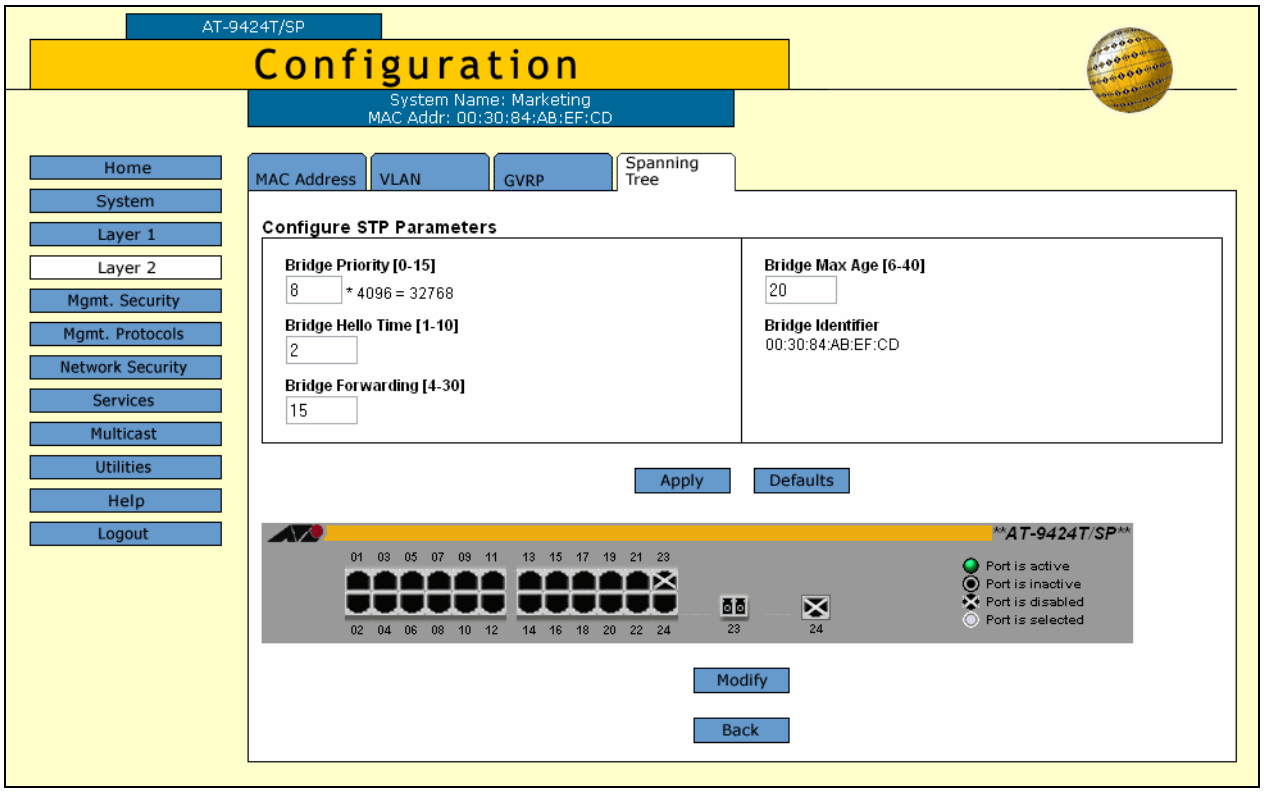

Figure 125. Configure STP Parameters Tab (Configuration)

Note
The Defaults button returns all STP settings to the default settings.

5. Configure the following parameters as necessary.

   Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of

4096, with 0 being the highest priority. For a list of the increments, refer to Table 6.

Table 6. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding Delay
The waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

In selecting a value for maximum age, the following rules must be observed:

MaxAge must be greater than (2 x (HelloTime + 1))

MaxAge must be less than (2 x (ForwardingDelay - 1))

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

6. After you have made the desired changes, click **Apply**.

7. To configure a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The STP Settings - Port(s) page is shown in Figure 126.

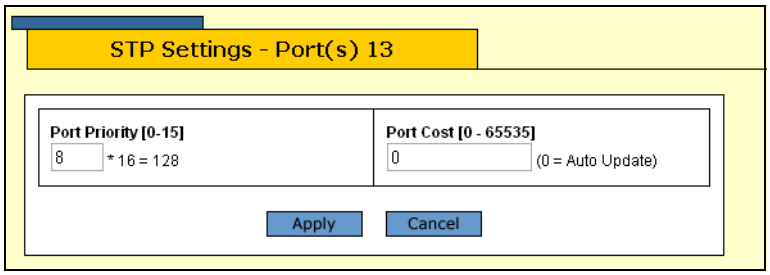

Figure 126. STP Settings - Port(s) Page

8. Configure the following parameters as necessary.

   Port Priority
   This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 7.

Table 7. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208

Table 7. Port Priority Value Increments (Continued)

Increment	Bridge Priority	Increment	Bridge Priority
6	96	14	224
7	112	15	240

Port Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 65,535. The default setting is Auto-detect, which sets port cost depending on the speed of the port. If you select Auto-Detect, the management software assigns a value of 100 if the port is operating at 10 Mbps, 10 for 100 Mbps, and 4 for one gigabit.

9. After you have configured the parameters, click **Apply**.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Note
A change to the port priority parameter takes effect immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying the STP Settings

To display the STP settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 127.

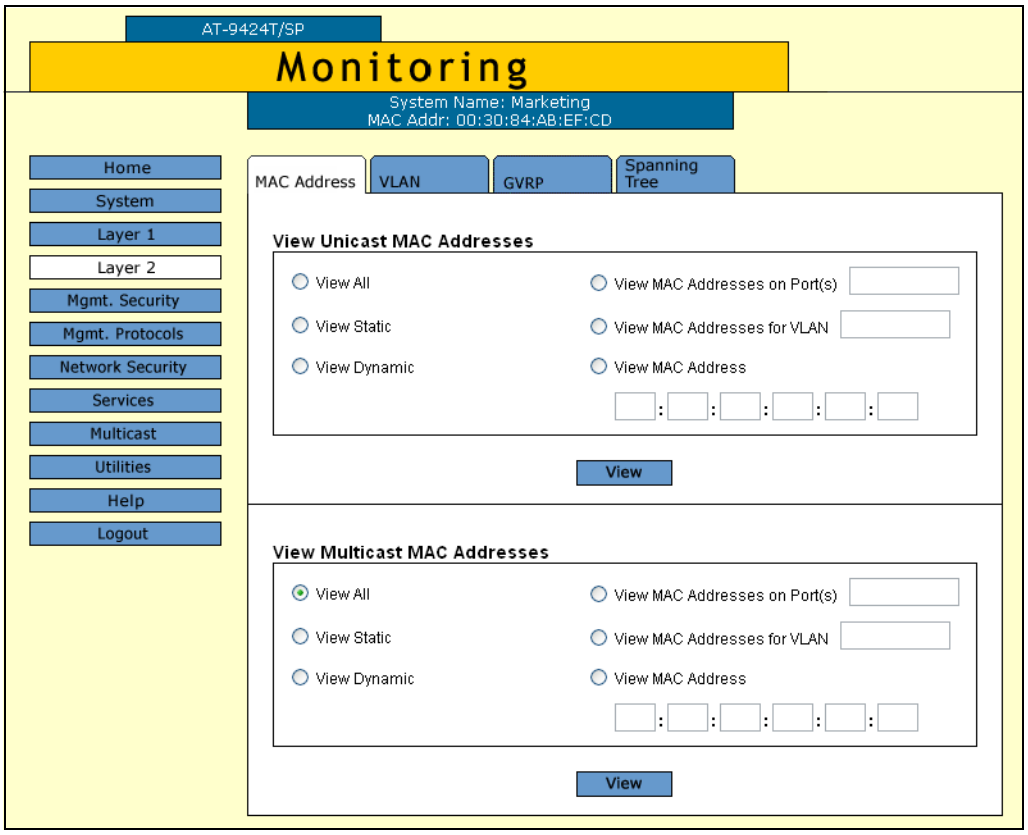

Figure 127. MAC Address Tab (Monitoring)

3. Select the **Spanning Tree** tab.

   The Spanning Tree tabs is shown in Figure 128.

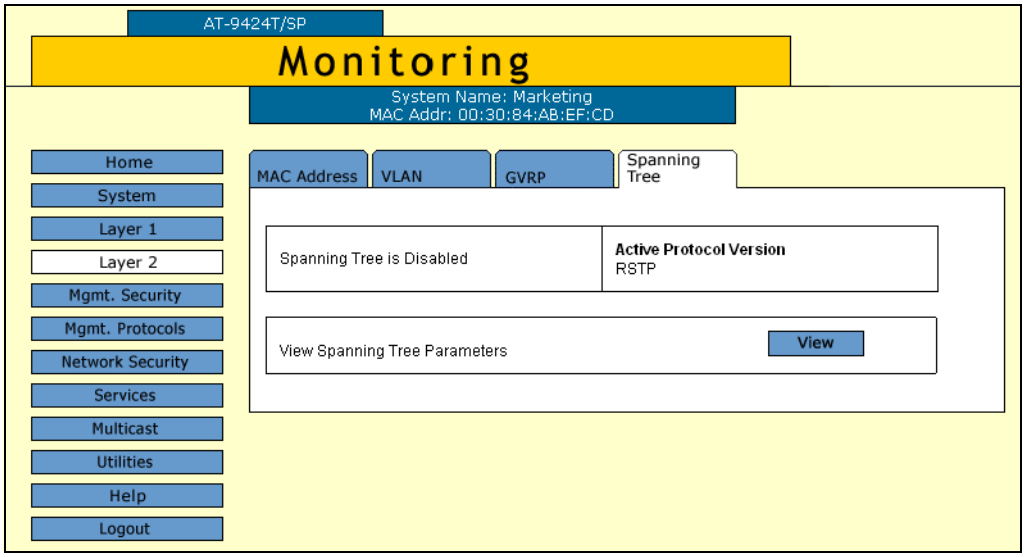

Figure 128. Spanning Tree Tab (Monitoring)

4. Click **View**.

   The Monitor STP Parameters tab is shown in Figure 129.

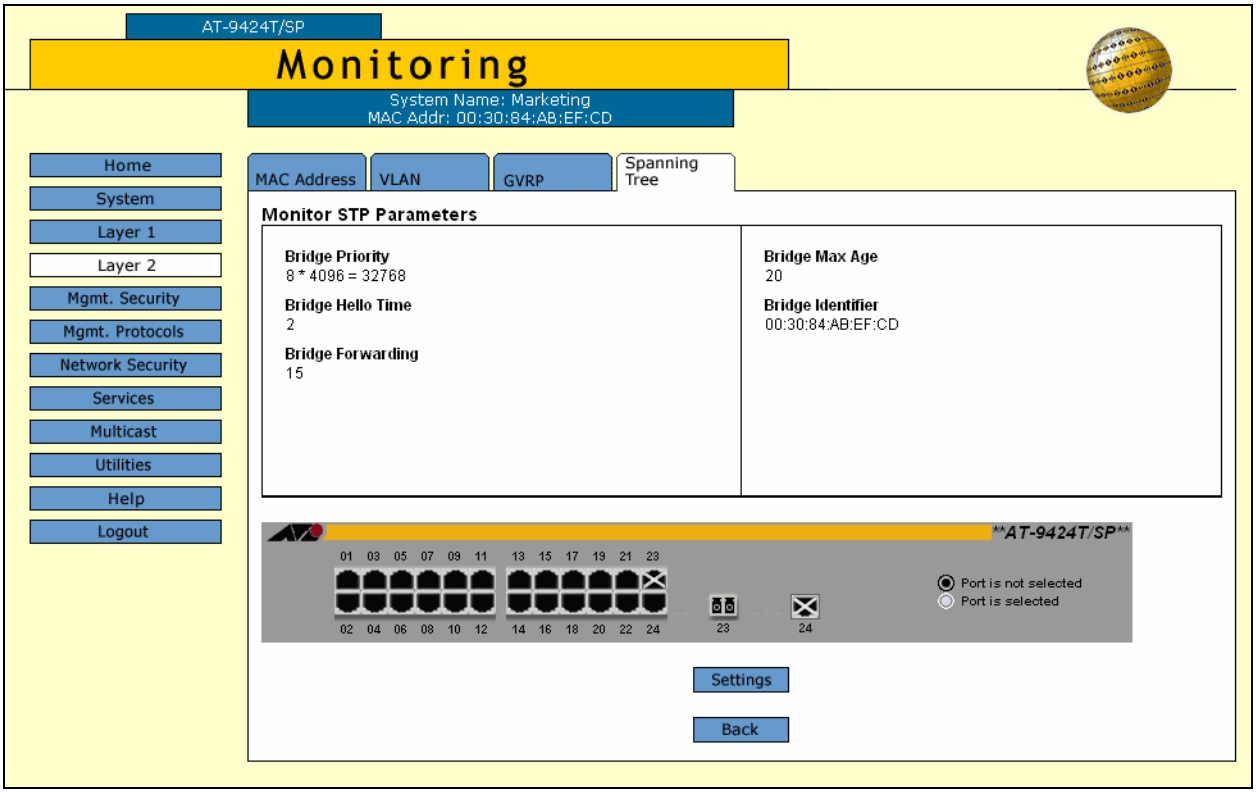

Figure 129. Monitor STP Parameters Tab (Monitoring)

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

   The STP Settings page is shown in Figure 130.

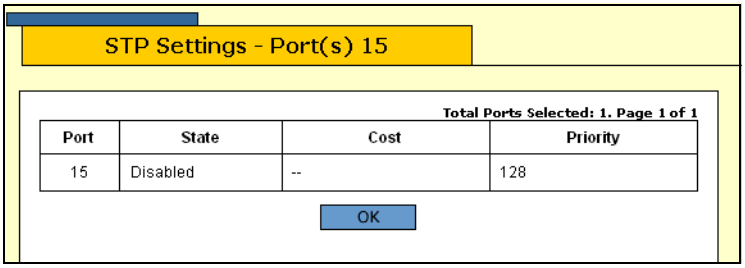

Figure 130. STP Settings Page

The STP Settings page displays a table that contains the following columns of information:

Port
Port number.

State
Current state of the port. The possible states are Enabled or Disabled.

Cost
Port cost of the port. The default is Auto-Update.

Priority
The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

6. Click **OK** to close the page.

Resetting STP to the Default Settings

To reset STP to the factory default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The Configure STP Parameters tab is shown in Figure 125 on page 305.

5. Click **Defaults**.

   The STP settings are returned to their default values.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring RSTP

Caution
The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

To configure RSTP, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

The Configure RSTP Bridge Parameters tab is shown in Figure 131.

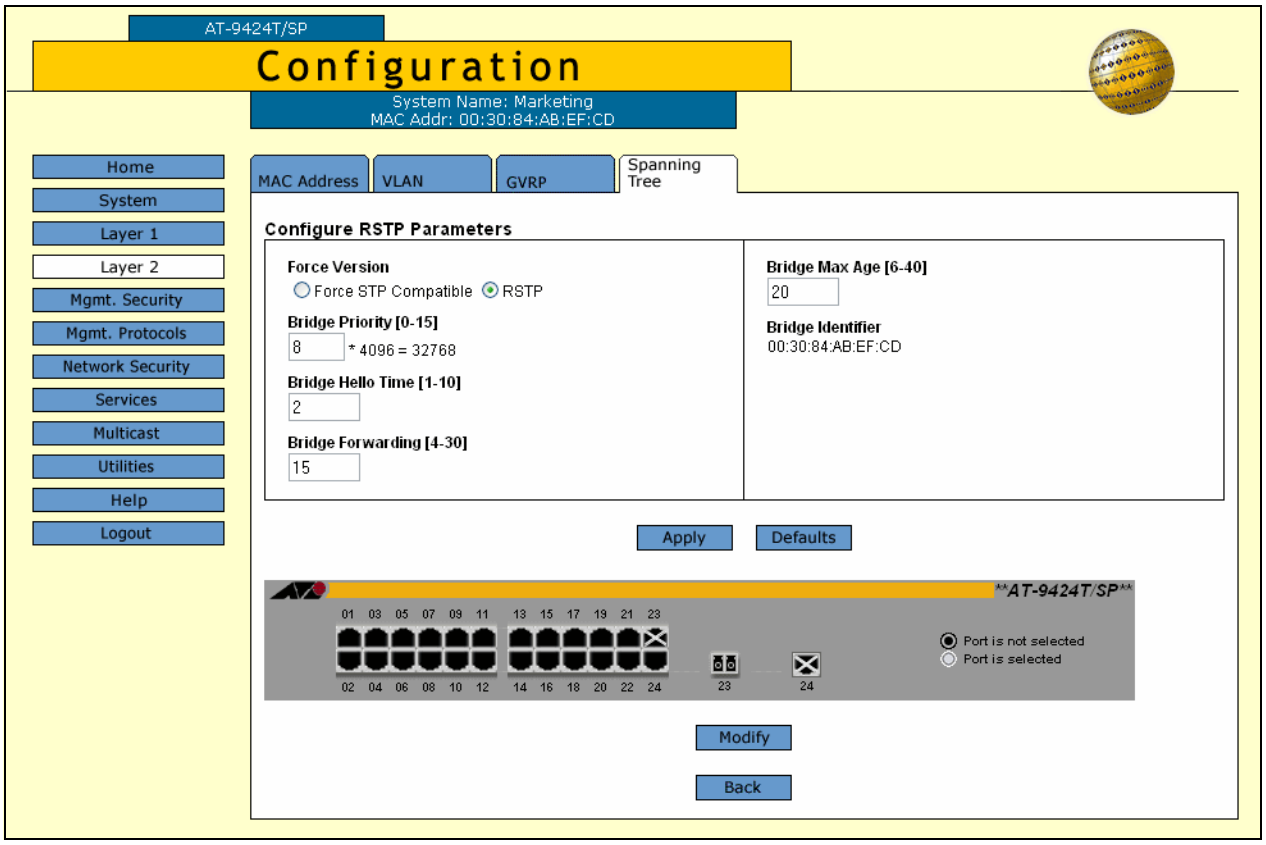

Figure 131. Configure RSTP Parameters Tab (Configuration)

5. Configure the following parameters as necessary.

Force Version
This selection determines whether the bridge operates with RSTP or in an STP-compatible mode. If you select RSTP, the bridge operates all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge operates in RSTP, using the RSTP parameter settings, but it sends only STP BPDU packets out the ports.

Bridge Priority
The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 6 on page 306.

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding
The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1)).

MaxAge must be less than (2 x (ForwardingDelay - 1))

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

6. After you have made your changes, click **Apply**.

7. To configure RSTP port settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The RSTP Settings - Port(s) page is shown in Figure 132.

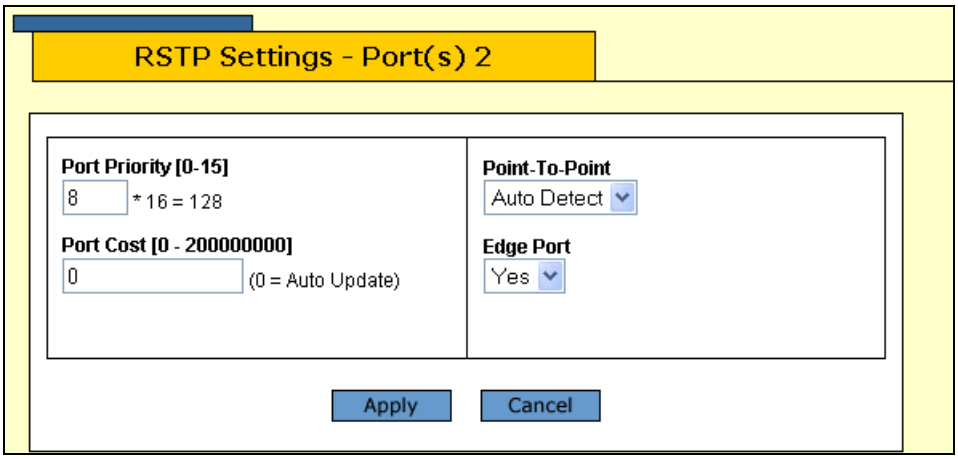

Figure 132. RSTP Settings - Port(s) Page

8. Configure the following parameters as necessary.

   Port Priority
   This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 7 on page 307.

   Port Cost
   The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20,000,000. The default setting is Automatic detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

   Point-to-Point
   This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 23, "Spanning Tree and Rapid Spanning Tree Protocols" in the *AT-S63 Management Software Menus Interface User's Guide*.

   Edge Port
   This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 23, "Spanning Tree and Rapid Spanning Tree Protocols" in the *AT-S63 Management Software Menus Interface User's Guide*.

9. After you have configured the parameters, click **Apply**.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Note
All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Resetting RSTP to the Default Settings

To reset RSTP to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select **Layer 2**.

   The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The Configure RSTP Bridge Parameters tab is shown in Figure 131 on page 313.

5. Click **Defaults**.

   The RSTP settings are returned to their default values.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying RSTP Settings

To display RSTP parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

3. The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 127 on page 309.

4. Select the **Spanning Tree** tab.

   The Spanning Tree tabs is shown in Figure 128 on page 309.

   This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP or RSTP, is active.

5. Click **View**.

   The Monitor RSTP Parameters tab is shown in Figure 133.

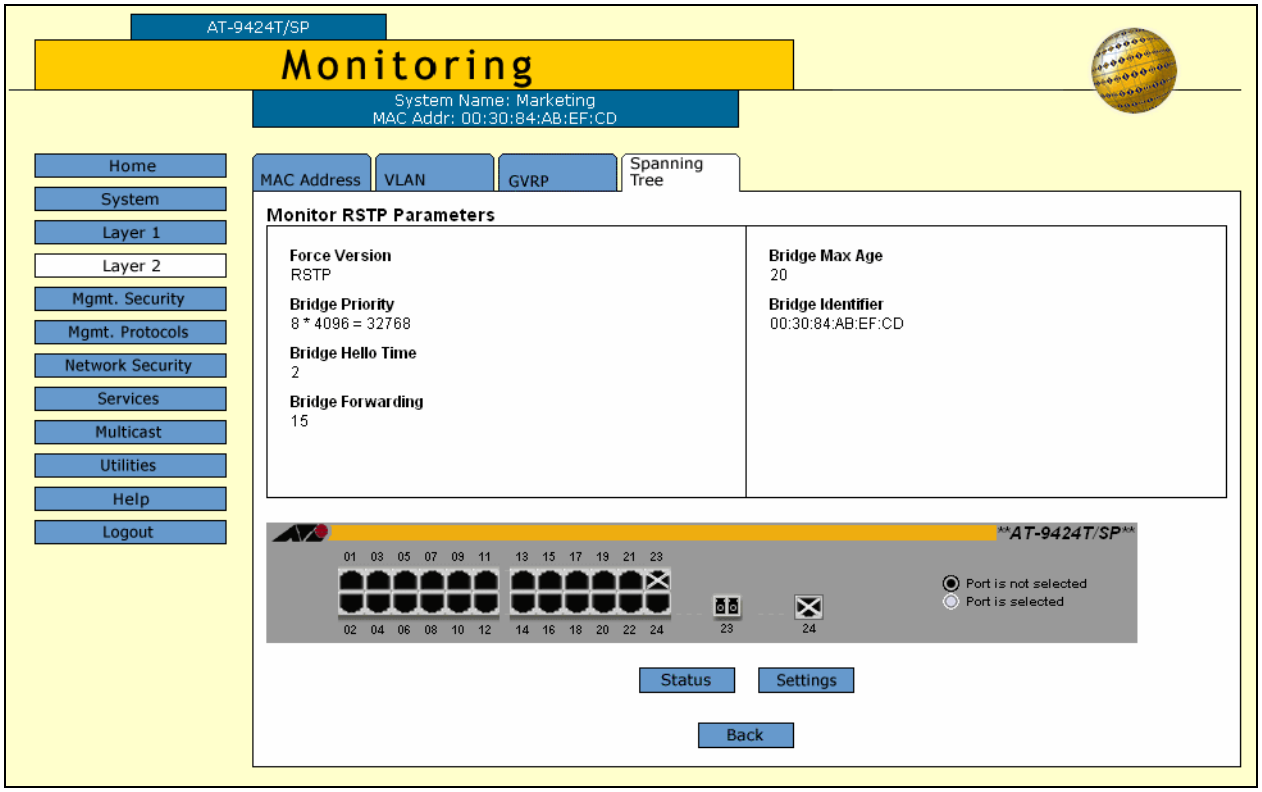

Figure 133. Monitor RSTP Parameters Tab (Monitoring)

6. To view port settings, click a port in the switch and click **Status** or **Settings**.

   The RSTP Settings page is shown in Figure 134.

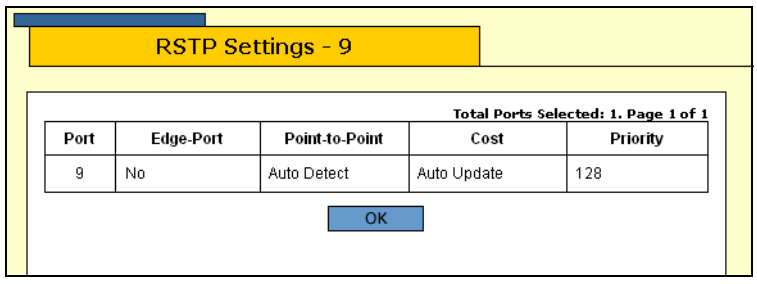

Figure 134. RSTP Settings Page

The RSTP Settings page displays a table that contains the following columns of information:

Port
The port number.

Edge-Port
Whether or not the port is operating as an edge port. The possible settings are Yes and No.

Point-to-Point
Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto Detect.

Cost
Port cost of the port. The default is Auto Update.

Priority
The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

7. Click **OK** to close the page.

Chapter 20

Multiple Spanning Tree Protocol

This chapter explains how to configure multiple spanning tree protocol (MSTP) parameters on an AT-9400 Series switch using a web browser management session. It contains the following procedures:

- ❒ “Enabling MSTP” on page 320
- ❒ “Configuring MSTP” on page 322
- ❒ “Creating, Deleting, or Modifying MSTI IDs” on page 326
- ❒ “Adding, Removing, or Modifying VLAN Associations to MSTIs” on page 330
- ❒ “Configuring MSTP Port Parameters” on page 333
- ❒ “Displaying the MSTP Port Configuration” on page 337
- ❒ “Displaying the MSTP Port Status” on page 340
- ❒ “Displaying the MSTP Port Status” on page 340
- ❒ “Resetting MSTP to the Default Settings” on page 342

Note
For background information on MSTP, refer to Chapter 24, “Multiple Spanning Tree Protocol,” in the *AT-S63 Management Software Menus Interface User’s Guide.*

Enabling MSTP

The AT-9400 Series switch can support the three spanning tree protocols STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. So before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol. After you select it, you can then enable or disable it.

To select MSTP as the active spanning tree protocol and to enable or disable it, perform the following procedure:

Note
Changing the active spanning tree protocol resets the switch.

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 123 on page 302.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 135.

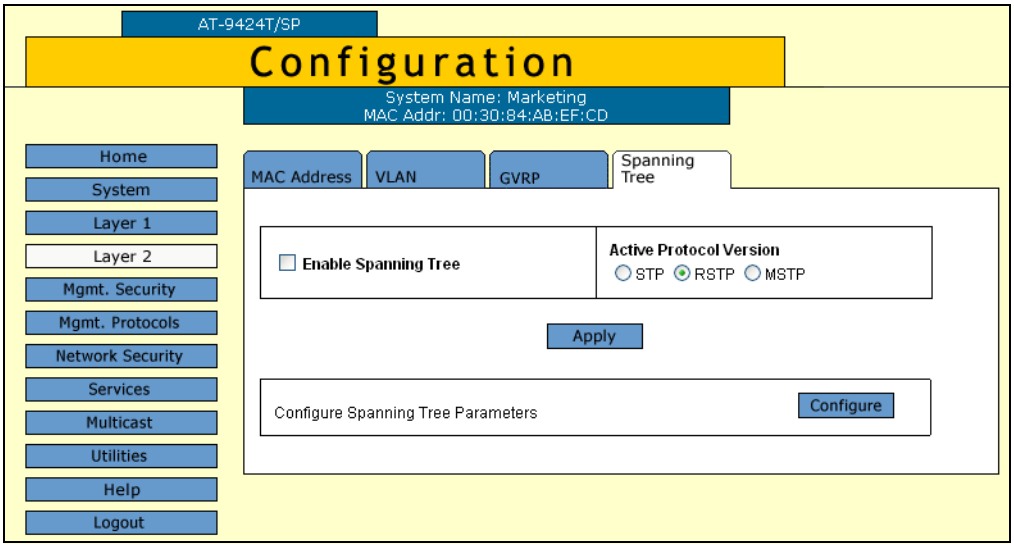

Figure 135. Spanning Tree Tab (Configuration)

Note
If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to Step 5.

4. To change the active spanning tree protocol on the switch, click **STP**, **RSTP**, or **MSTP** in the Active Protocol Version section of the tab. The default is RSTP.

Note
Only one spanning tree protocol can be active on the switch at a time.

5. To enable or disable the active spanning tree protocol on the switch, click the **Enable Spanning Tree** check box. A check indicates that the spanning tree is enabled while no check indicates that spanning tree is disabled. The default is disabled.

6. Click **Apply**.

Note
If you changed the active spanning tree protocol, the switch resets and your management session is ended. To continue managing the switch, you must restart your management session after the switch is finished reloading the AT-S63 management software.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

8. If you activated STP, go to "Configuring STP" on page 304. If you activated RSTP go to "Configuring RSTP" on page 312. If you activated MSTP, go to "Configuring MSTP" on page 322.

Configuring MSTP

This section contains the following procedures:

- ❒ “Configuring MSTP Parameters,” next
- ❒ “Configuring the CIST Priority” on page 325
- ❒ “Creating, Deleting, or Modifying MSTI IDs” on page 326
- ❒ “Adding, Removing, or Modifying VLAN Associations to MSTIs” on page 330
- ❒ “Configuring MSTP Port Parameters” on page 333

Note
MSTP must be selected as the active spanning tree protocol on the switch before you can configure it. For instructions on selecting the active spanning tree, refer to “Enabling MSTP” on page 320.

Note
When MSTP is enabled, the GVRP tab is not shown on the Configuration or Monitoring Layer 2 page.

Configuring MSTP Parameters

To configure MSTP parameters, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136.

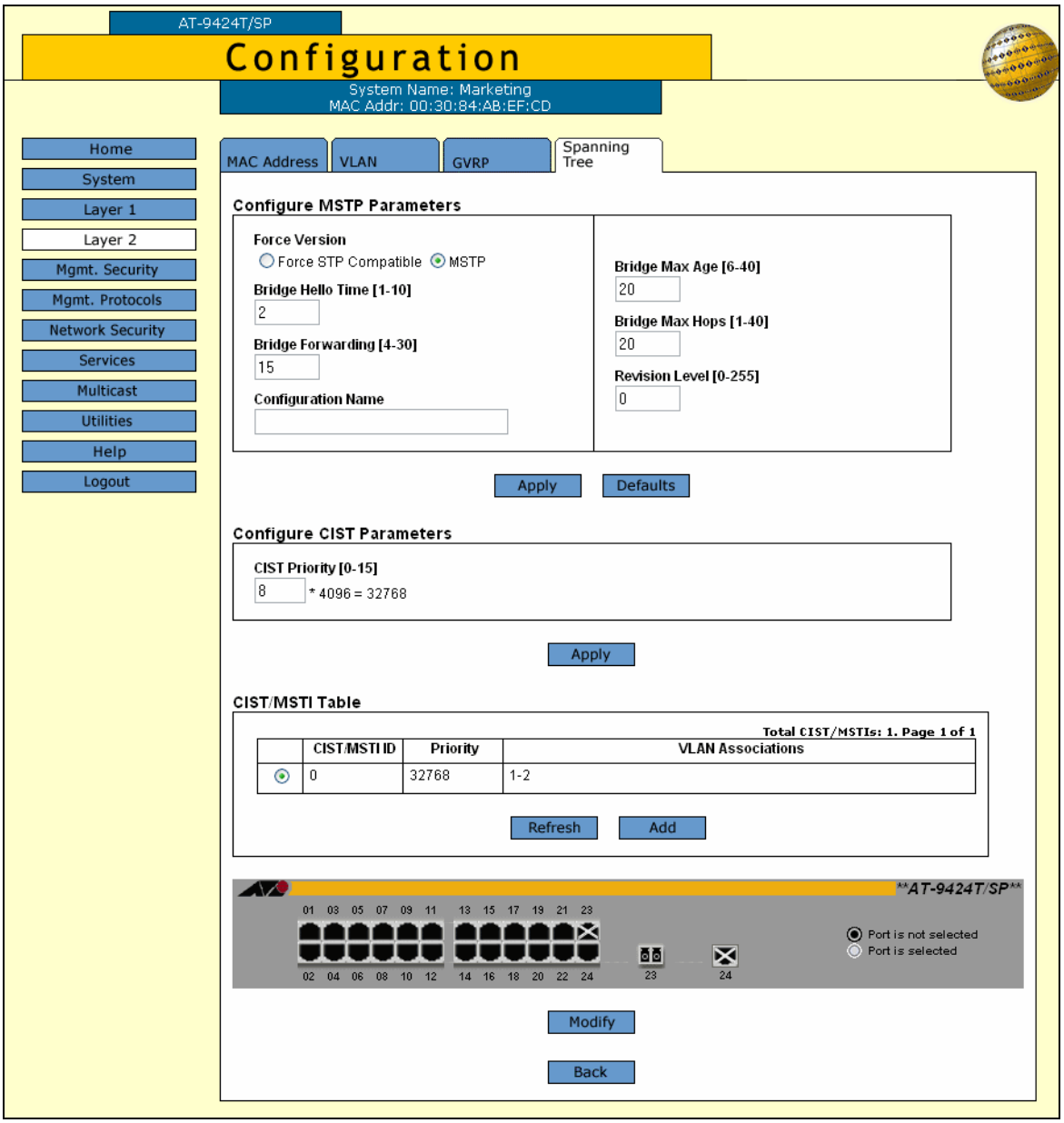

Figure 136. Configure MSTP Parameters Tab (Configuration)

Note

This procedure explains the Configure MSTP Parameters section of the page. The CIST/MSTI Table is explained in "Adding, Removing, or Modifying VLAN Associations to MSTIs" on page 330. The graphic image of the switch is described in "Configuring MSTP Port Parameters" on page 333.

Configure the following parameters as necessary.

Force Version
This selection determines whether the bridge operates with MSTP or in an STP-compatible mode. If you select MSTP, the bridge operates all ports in MSTP, except those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. The default is MSTP.

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of the network.

Bridge Forwarding
The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is from 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Configuration Name
The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case sensitive, must be the same on all bridges in a region. Examples of a configuration name include Sales Region and Production Region.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1))

MaxAge must be less than (2 x (ForwardingDelay - 1))

Bridge Max Hops
MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. After the counter reaches zero, the BPDU is deleted.

Revision Level
The revision level of an MSTP region. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 255.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

   Or, proceed to the next procedure to configure the CIST priority.

Configuring the CIST Priority

To configure the CIST priority, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the Configure CIST Parameters section, set the **CIST Priority**, the priority number for the bridge.

   This number is used to determine the root bridge of the bridged network. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Creating, Deleting, or Modifying MSTI IDs

To create, delete, or modify MSTI IDs, perform one of the following procedures.

Creating an MSTI ID

To create an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the CIST/MSTI Table section of the tab, click **Add**.

   The Add New MSTI page is shown in Figure 137.

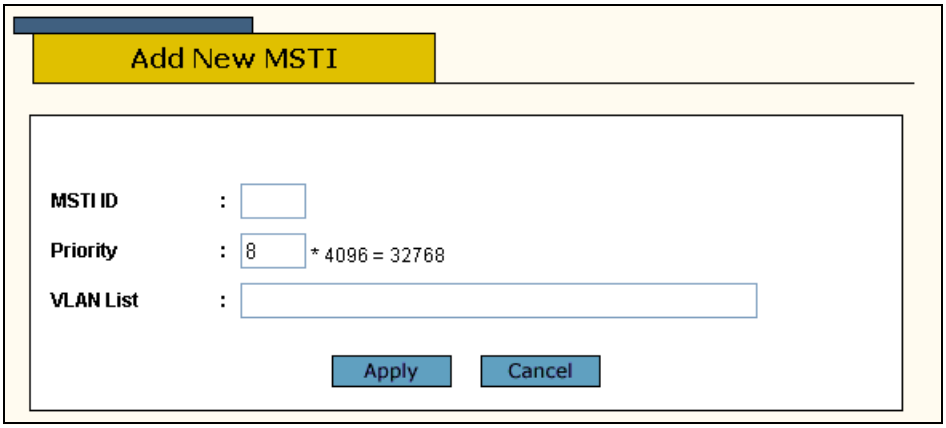

Figure 137. Add New MSTI Page

6. In the MSTI ID field, enter a new MSTI ID. The range is 1 to 15.

7. In the Priority field, enter an MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. This parameter is used in selecting a regional root for the MSTI. For a list of the increments, refer to Table 6, "Bridge Priority Value Increments" on page 306. The default is 0.
8. Click **Apply**.
9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
10. Repeat this procedure to create more MSTI IDs.

Deleting an MSTI ID

To delete an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID you want to delete. You can select only one MSTI ID at a time.
6. Click **Remove**.
7. A confirmation prompt is displayed.
8. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure:
9. If you select OK, the MSTI is deleted and VLANs associated with it are returned to CIST, which has an ID of 0.

Modifying an MSTI ID

To modify an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID you want to modify. You can select only one MSTI ID at a time. You cannot modify CIST.

6. Click **Modify**.

   The Modify MSTI page is shown in Figure 138.

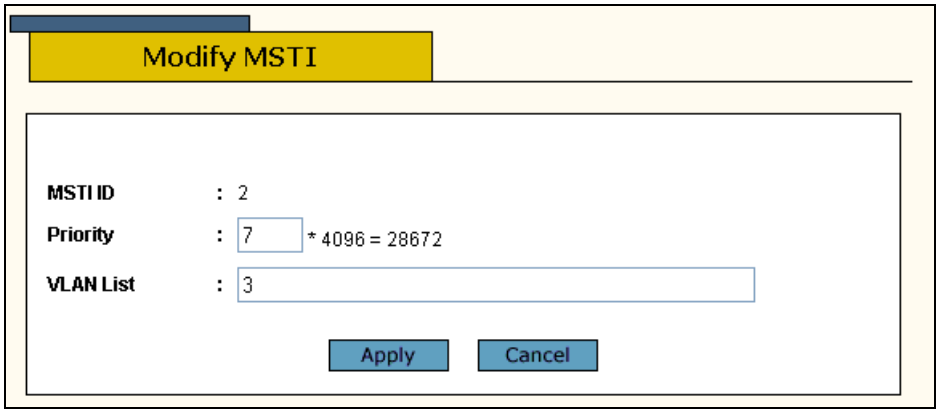

Figure 138. Modify MSTI Page

7. In the Priority field, enter a new MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. For a list of the increments, refer toTable 6, “Bridge Priority Value Increments” on page 306. The default is 0.

8. Click **Apply**.

9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

10. Repeat this procedure to modify more MSTI IDs.

Adding, Removing, or Modifying VLAN Associations to MSTIs

This section explains how to add or remove VLANs associated to MSTI IDs.

Adding a VLAN Association

To add a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, enter the VIDs of the VLANS to be associated with this MSTI. You can specify more than one VID at a time (for example, 2,4,7).

6. Click Apply.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

   Or, proceed to the next procedure to configure the CIST priority.

Removing a VLAN Association

To remove a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, remove the VIDs of the VLANS that you no longer want to be associated with this MSTI. You can specify more than one VID at a time (for example, 2,4,7).

6. Click Apply.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

   Or, proceed to the next procedure to configure the CIST priority.

Modifying a VLAN Association

To modify a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, modify the VIDs of the VLANS that you no longer want to be associated with this MSTI. You can specify more than one VID at a time (e.g., 2,4,7).

6. Click Apply.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 135 on page 320.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. In the diagram of the switch at the bottom of the MSTP Spanning Tree Expanded page, click the ports you want to configure. You can select more than one port at a time.

6. Click **Modify**.

   The MSTP Settings - Port(s) page is shown in Figure 139.

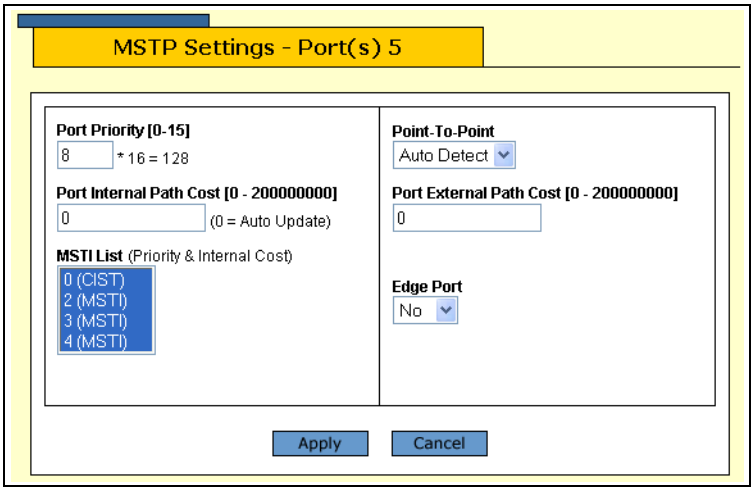

Figure 139. MSTP Settings - Port(s) Page

7. Configure the following parameters as necessary.

   The port parameters can be divided into two groups: generic parameters and MSTI-specific parameters. A generic port parameter is set just once on a port and applies to all of a port's MSTIs assignments. Generic parameters are:

   - ❒ External path cost
   - ❒ Point-to-point port
   - ❒ Edge port

   An MSTI-specific parameter can be set on a per MSTI basis. This means that you can assign a different value to a MSTI-specific parameter for each spanning tree instance where a port is a member. These parameters are:

   - ❒ Internal path cost
   - ❒ Port priority

   When setting an MSTI-specific parameter, use the MSTI List in the window to select the intended MSTI. It should be noted that the MSTI List shows all of the spanning tree instances on the switch, and not just those where the selected port is currently a member. If you select an MSTI where the port is not a member, you can pre-configure the parameter in the event you later add the port as a member of the MSTI through a VLAN assignment.

   Port Priority
   This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value is 128). For a list of the increments, refer to Table 7, "Port Priority Value Increments" on page 307.

   Port Internal Path Cost
   The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Table 8 lists the MSTP port cost with Auto Update when a port is not part of a port trunk.

   Table 8. MSTP Auto Update Port Internal Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 9 lists the MSTP port costs with Auto Update when the port is part of a port trunk.

Table 9. MSTP Auto Update Port Trunk Internal Path Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

MSTI List
The MSTIs defined on the switch. You can use this list when setting the port priority and port internal path cost parameters to assign different values to a port for each MSTI when the port is a member. Before setting priority or internal path cost, select the appropriate MSTI where you want the new setting to be applied on the port. The default is all MSTIs on the switch.

The MSTI List shows all of the spanning tree instances on the switch, and not just those where the selected port is currently a member. If you select an MSTI where the port is not a member, you can pre-configure the parameter in the event you later add the port as a member of the MSTI through a VLAN assignment.

Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 23, "Spanning Tree and Rapid Spanning Tree Protocols" in the *AT-S63 Management Software Menus Interface User's Guide*.

Port External Path Cost
The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. Table 10 lists the MSTP port costs with the Auto setting when the port is not a member of a trunk.

Table 10. MSTP Auto External Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 11 lists the MSTP port costs with the Auto setting when the port is part of a port trunk.

Table 11. MSTP Auto External Path Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

Edge Port
This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 23, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Menus Interface User’s Guide*.

8. After configuring the parameters, click **Apply**.
9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
10. Repeat this procedure to configure MSTP parameters for other switch ports.

Displaying the MSTP Port Configuration

To display the MSTP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 124 on page 303.

   This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP, RSTP, or MSTP is active.

4. Click **View**.

The MSTP Parameters tab is shown in Figure 140.

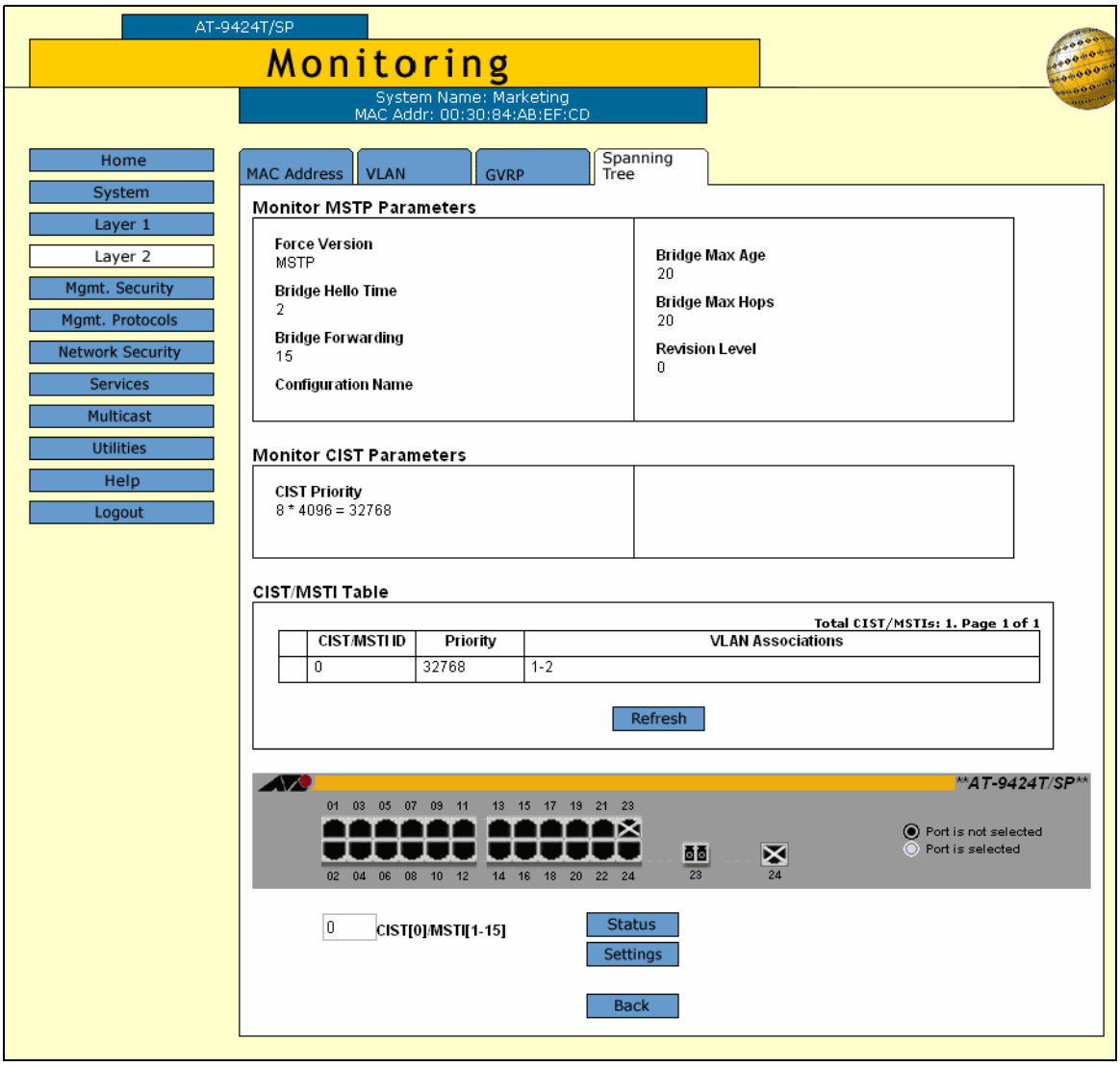

Figure 140. Monitor MSTP Parameters Tab (Monitoring)

5. Click a port in the switch and click **Settings**. You can select more than one port.

   The MSTP Settings - Port (s) page is shown in Figure 141.

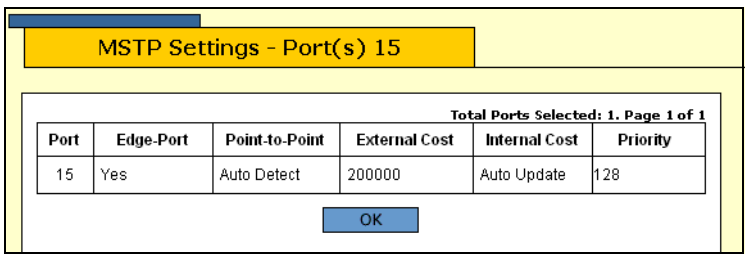

Figure 141. MSTP Settings - Port(s) Page

The MSTP Settings page displays a table that contains the following columns of information:

Port
The port number.

Edge-Port
Whether or not the port is functioning as an edge port. The possible settings are Yes and No.

Point-to-Point
Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

External Cost
The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP.

Internal Cost
The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The possible settings are:

Auto-detect - Port cost is automatically set depending on the speed of the port.

Default values - 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge.

6. Click **OK** to close the page.

Displaying the MSTP Port Status

To display MSTP port status, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Monitoring Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 27 on page 98.

3. Select the **Spanning Tree** tab.

   The Monitoring Spanning Tree tab for the active protocol, MSTP, is shown in Figure 140

4. Click a port in the switch and click **Status**. You can select more than one port.

   The MSTP Port Status - Port(s) page is shown in Figure 142.

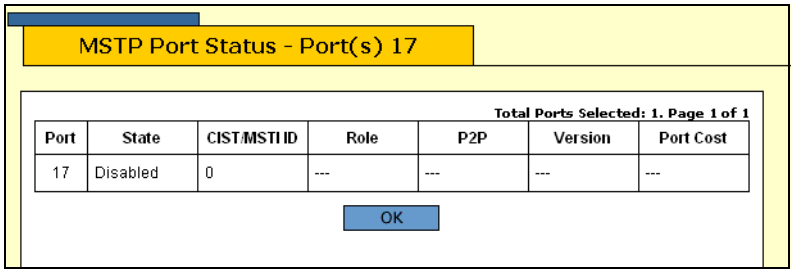

Figure 142. MSTP Port Status - Port(s) Page

The MSTP Port Status page displays a table that contains the following columns of information:

Port
The port number.

State
The MSTP state of the port. The possible states are:

Discarding - The port is discarding received packets and is not submitting forwarded packets for transmission.

Learning - The port is enabled for receiving, but not forwarding packets.

Forwarding - Normal operation.

Disabled - The port has not established a link with its end node.

Role
The MSTP role of the port. The possible roles are:

Root - The port that is connected to the root switch, directly or through other switches, with the least path cost.

Alternate - The port offers an alternate path in the direction of the root switch.

Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch.

Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called "master" when the CIST role is "root."

P2P
Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

Version
Whether the port is operating in MSTP mode or STP-compatible mode.

Internal Port Cost
The port cost when the port is connected to a bridge in the same MSTP region.

5. Click **OK** to close the page.

Resetting MSTP to the Default Settings

To reset MSTP to the factory default settings, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 135 on page 320.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 136 on page 323.

5. Click **Defaults**.

   The MSTP settings are returned to their default values.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Section V

Virtual LANs

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- Chapter 21, “Port-based and Tagged VLANs” on page 345
- Chapter 22, “GARP VLAN Registration Protocol” on page 359
- Chapter 23, “Protected Ports VLANs” on page 375

Chapter 21

Port-based and Tagged VLANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs. This chapter also explains how to select a multiple VLAN mode.

This chapter contains the following sections:

- ❒ “Creating a New Port-Based or Tagged VLAN” on page 346
- ❒ “Modifying a VLAN” on page 350
- ❒ “Deleting a VLAN” on page 352
- ❒ “Selecting a VLAN Mode” on page 353
- ❒ “Displaying VLANs” on page 355
- ❒ “Specifying a Management VLAN” on page 357

Note
For background information on port-based and tagged VLANs, as well as the management VLAN, refer to Chapter 25, “Port-based and Tagged VLANs,” in the *AT-S63 Management Software Menus Interface User’s Guide*. For more information about the multiple VLAN modes, refer to Chapter 27, “Multiple VLAN Modes,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a New Port-Based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 123 on page 302.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143.

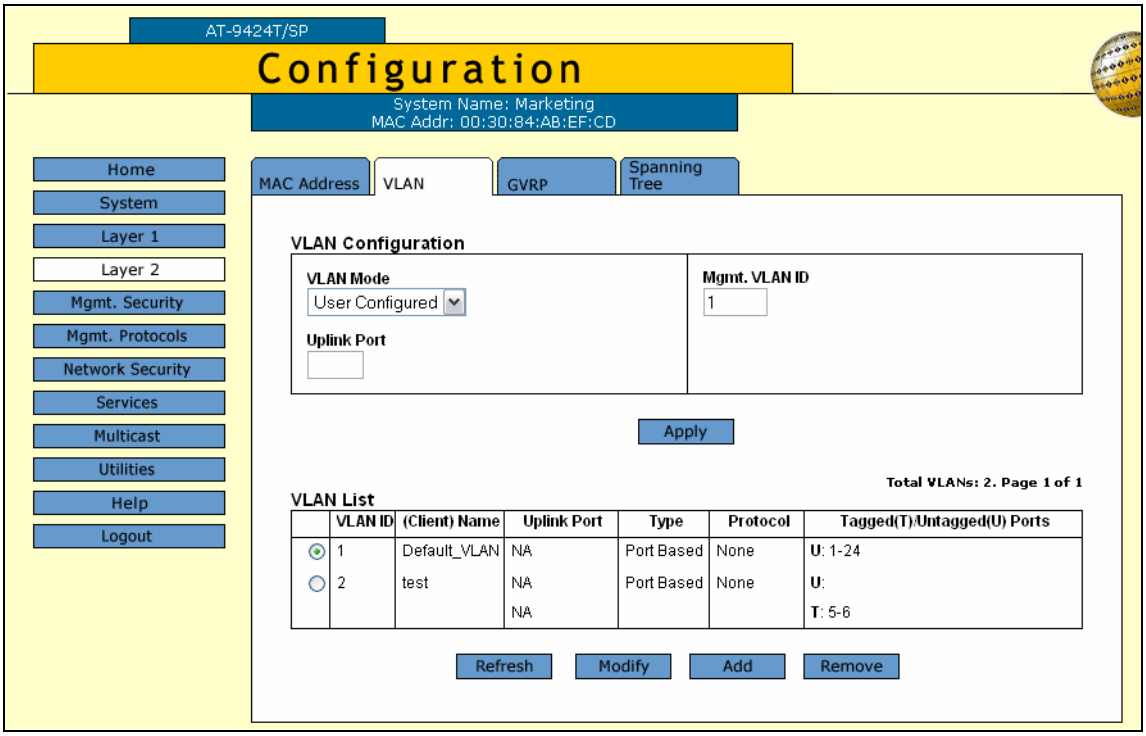

Figure 143. VLAN Tab (Configuration)

Note
The Modify and Remove buttons are not shown in the tab if the only VLAN on the switch is the Default_VLAN.

The VLAN Mode and Uplink Port options are explained in "Selecting a VLAN Mode" on page 353. The Mgmt. VLAN ID option is explained in "Specifying a Management VLAN" on page 357.

The tab displays an existing VLANs on the switch.

4. To add a new VLAN, click **Add**.

   The Add New VLAN page is shown in Figure 144.

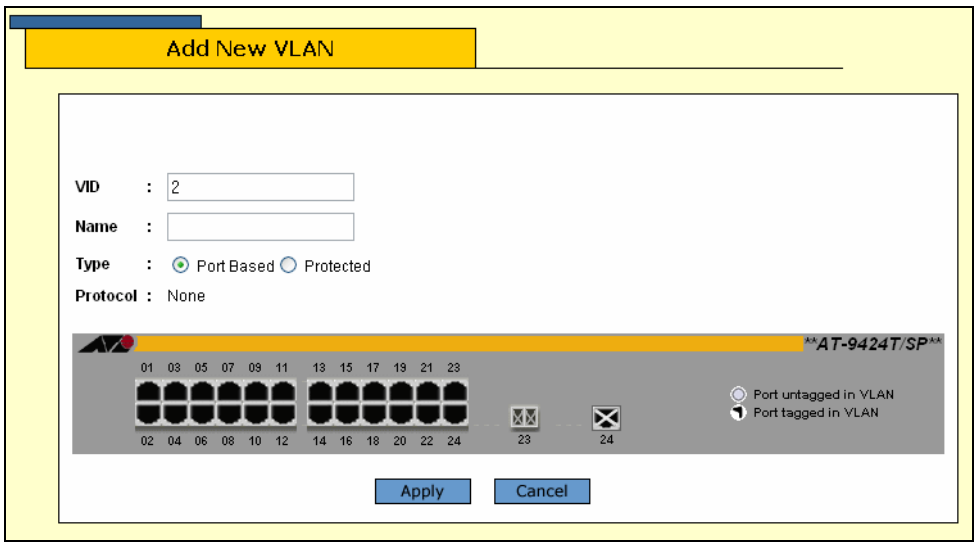

Figure 144. Add New VLAN Page

5. Configure the following parameters as necessary.

   VID
   Enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

   If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, you should assign the Sales VLAN on each switch the same VID value.

   Note
   A VLAN must have a VID.

   It is important to note that the switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-9400 Series switch to a network that already contains VLANs that use VIDs 2 through 24, the AT-S63 management software still uses VID 2 as the

default value when you create the first VLAN on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Name
Specify a name for the new VLAN.

The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that are part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

If the VLAN is unique in your network, then the name should be unique as well. If the VLAN is part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

Note
A VLAN must be assigned a name.

Type
Select **Port Based** as the Type. This is the default setting. This is the correct setting when creating a port-based or tagged VLAN.

Note
The Type selection of Protected is used to create a protected ports VLAN, as explained in Chapter 23, “Protected Ports VLANs” on page 375.

6. To select the ports for the VLAN, click on the appropriate ports in the switch image.

   Clicking repeatedly on a port toggles the port through the following possible settings:

   Untagged port

   Tagged port

   Port is not a member of the VLAN

7. Click **Apply**.

   Note
   Any untagged ports that you assign to the new VLAN are automatically removed from their current untagged VLAN assignment.

   The new user-configured VLAN is now ready for network operations.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a VLAN

This procedure explains how to add or remove ports from a VLAN. When modifying a VLAN, note the following:

- ❒ You cannot change the VID of a VLAN.
- ❒ You cannot change the name of a VLAN from a web browser management session, but you can from a local or Telnet session.
- ❒ You cannot modify VLANs when the switch is operating in one of the multiple VLAN modes.

To modify a VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

4. Click the button next to the name of the VLAN you want to modify.

5. Click **Modify**.

   The Modify VLAN page for the VLAN is displayed.

6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image.

   Clicking repeatedly on a port toggles the port through the following possible settings:

   Untagged port

   Tagged port

   Port is not a member of the VLAN

7. Click **Apply**.

Note
Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN leaves the port as an untagged member of no VLAN.

The modified VLAN is now ready for network operations.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a VLAN

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

4. Click the button next to the name of the VLAN you want to delete. (You cannot delete the Default_VLAN.)

5. Click **Remove**.

   A confirmation prompt is displayed.

6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure:

   If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Selecting a VLAN Mode

The AT-S63 management software features three VLAN modes:

- Port-based and tagged VLAN Mode (default mode)
- IEEE 802.1Q-compliant Multiple VLAN Mode
- Non-IEEE 802.1Q compliant Multiple VLAN Mode

For background information on port-based and tagged VLANs, refer to Chapter 25, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*. For information on the multiple VLAN modes, refer to Chapter 27, "Multiple VLAN Modes," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note
Any port-based or tagged VLANs that you may have created are not retained when you change the VLAN mode from the user configured mode to a multiple VLAN mode and, at some point, reset the switch. The user configured VLAN information is lost and you must recreate the information if you later return the switch to the user configured VLAN mode.

To select a VLAN mode for the switch, perform the procedure below:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

4. In the VLAN Mode section, select a VLAN mode. Only one mode can be active on the switch at a time. The modes are:

   User Configured - Port-based and tagged VLAN Mode

   Multiple - Non-IEEE 802.1Q-compliant Multiple VLAN Mode

   Multiple 802.1Q - IEEE 802.1Q-compliant Multiple VLAN Mode

5. If you select one of the multiple VLAN modes, specify an uplink port in the Uplink Port field. This port functions as the uplink port for the VLANs. The default is port 1.

6. Click **Apply**.

   The new mode is automatically activated on the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying VLANs

To display the current VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

3. The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

4. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 145.

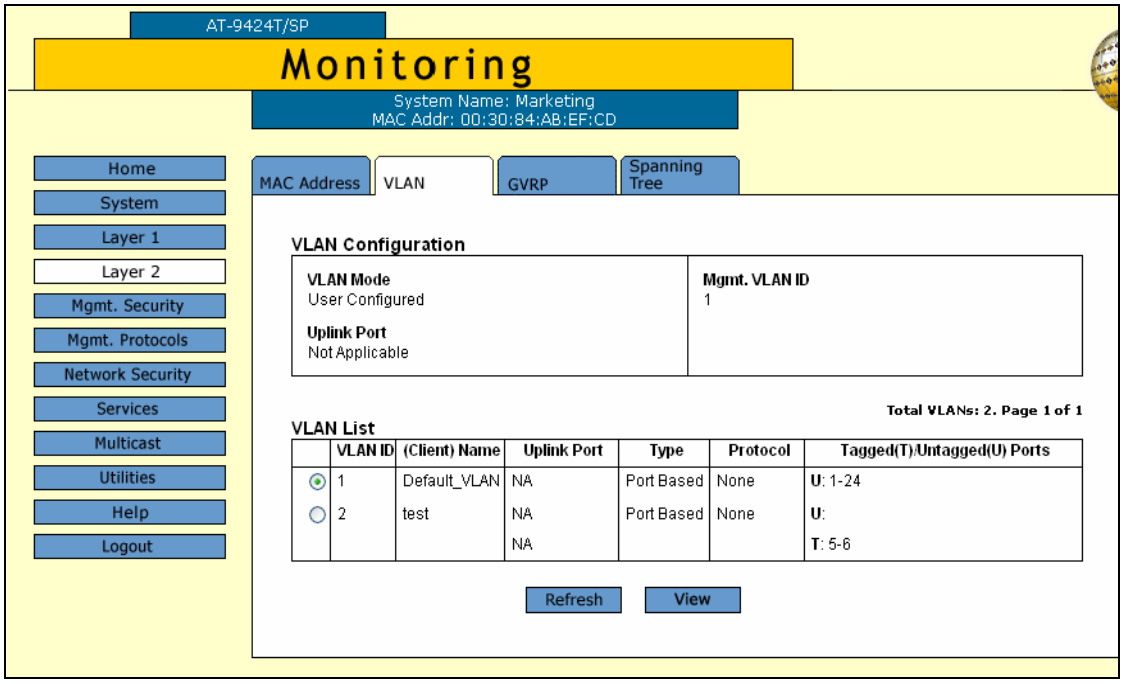

Figure 145. VLAN Tab (Monitoring)

The upper part of the tab displays the following information:

Mode
The VLAN mode. The possible settings are:

User Configured - This mode supports port-based and tagged VLANs.

Multiple 802.1Q - The IEEE 802.1Q-compliant multiple VLAN mode.

Multiple - The non-IEEE 802.1Q-compliant multiple VLAN mode.

Management VLAN ID
VLAN ID of the management VLAN.

The lower part of the tab displays a table that contains the following columns of information:

VLAN ID
The VID number assigned to the VLAN.

(Client) Name
The name of the VLAN. If the switch is operating in one of the multiple VLAN modes, the names of the VLANs start with “Client,” with the exception of the VLAN containing the uplink port, which starts with “Uplink.”

Uplink Port
This column contains “NA,” meaning Not Applicable, for tagged and port-based VLANs. For a protected ports VLAN, this column contains the uplink port(s) for the port groups. A tagged uplink port is designated with a “T” and an untagged uplink port has a “U.” If the switch is operating in one of the two multiple VLAN modes this column displays the port that is functioning as the uplink port for the other ports on the switch.

VLAN Type
The VLAN type. The possible settings are:

Port Based - The VLAN is a port-based or tagged VLAN.

GARP - The VLAN was automatically created by GARP.

Protocol
The protocol associated with this VLAN. The possible settings are:

Blank - The VLAN is a port-based or tagged VLAN.

GARP - The VLAN is a dynamic GVRP VLAN or the port is a dynamic GVRP port of a static VLAN.

Tagged(T)/Untagged(U) Port
Lists the ports of the VLAN. Tagged ports are designated with a “T” and untagged ports with a “U.”

Specifying a Management VLAN

The management VLAN is the VLAN through which an AT-9400 Series switch expects to receive management packets. This VLAN is important if you are managing a switch remotely or using the enhanced stacking feature of the switch. For more details about specifying a management VLAN, see Chapter 25, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note
You cannot specify a management VLAN when the switch is operating in a multiple VLAN mode.

To specify the management VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 94.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

4. For the Mgmt. VLAN ID parameter, enter the VID of the VLAN on the switch that you want to function as the management VLAN. The VLAN must already exist on the switch. The default is 1, which is the VID of the Default_VLAN.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Chapter 22

GARP VLAN Registration Protocol

This chapter contains instructions on how to configure GARP VLAN Registration Protocol (GVRP). This chapter contains the following procedures:

- ❒ “Configuring GVRP” on page 360
- ❒ “Enabling or Disabling GVRP on a Port” on page 362
- ❒ “Displaying the GVRP Configuration” on page 363
- ❒ “Displaying the GVRP Port Configuration” on page 365
- ❒ “Displaying the GVRP Database” on page 366
- ❒ “Displaying the GVRP State Machine” on page 367
- ❒ “Displaying the GVRP Counters” on page 370
- ❒ “Displaying the GIP Connected Ports Ring” on page 373

Note
For background information on GVRP, refer to Chapter 26, “GARP VLAN Registration Protocol,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring GVRP

To configure GVRP, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 146.

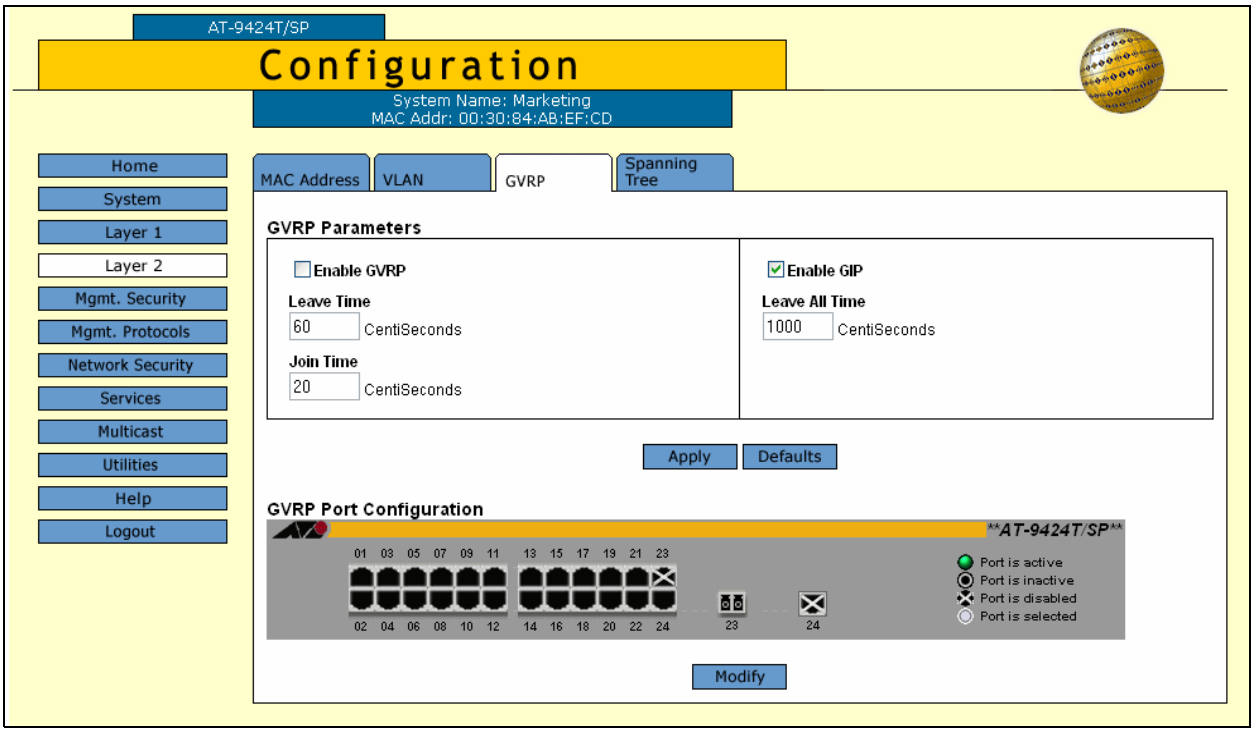

Figure 146. GVRP Tab (Configuration)

4. In the GVRP Parameters section, configure the following parameters as necessary.

   Enable GVRP
   Click to enable or disable GVRP.

Leave Time
Use this parameter to specify the leave time. The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time
Use this parameter to specify the join time. The range is 10 to 60 centiseconds and the default is 20 centiseconds.

Enable GIP
Click to enable GIP, which is required to propagate VLAN information among the ports of the switch.

Leave All Time
The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

5. Click **Apply**.

   Configuration changes are immediately activated on the switch.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Enabling or Disabling GVRP on a Port

To enable or disable GVRP on a port, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 25 on page 94.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 146 on page 360.

4. In the GVRP Port Configuration section, click the ports that you want to configure.

5. Click **Modify**.

   The GVRP Port Configuration page is shown in Figure 147.

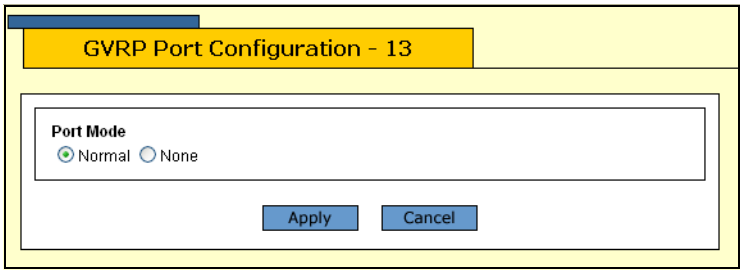

Figure 147. GVRP Port Configuration Page

6. Click **Normal** to have the port propagate GVRP information, or **None** to prevent processing GVRP information and transmitting PDUs.

7. Click **Apply** to save the change, or **Cancel** to cancel.

Displaying the GVRP Configuration

To display the GVRP configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 148.

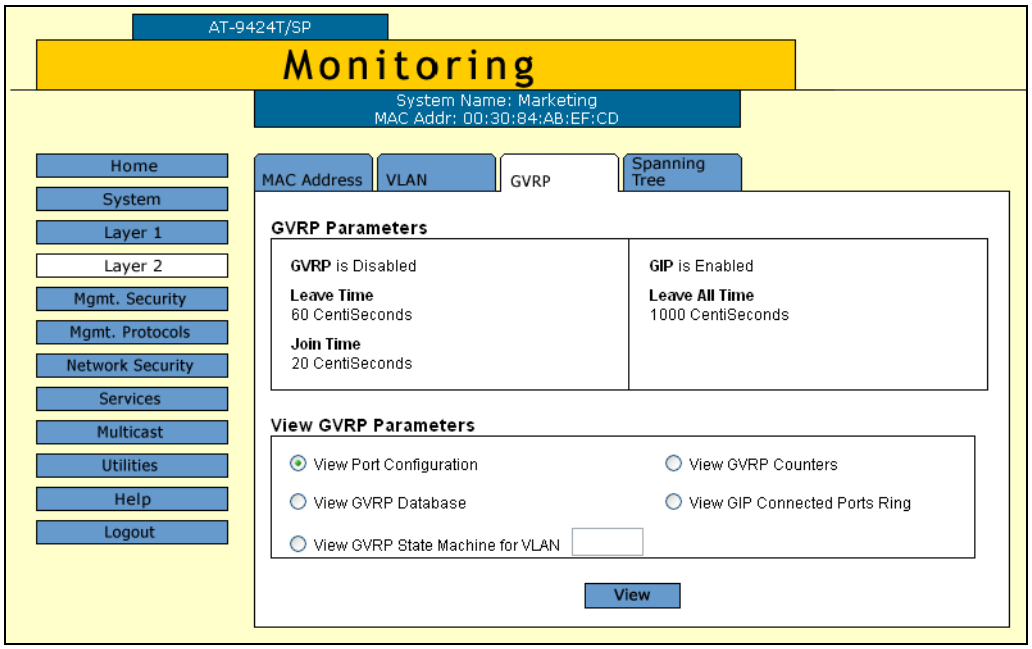

Figure 148. GVRP Tab (Monitoring)

The GVRP Parameters section provides the following information:

GVRP
The GVRP status, Enabled or Disabled.

Leave Time
The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time
The range is 10 to 60 centiseconds and the default is 20 centiseconds.

GIP
The GIP status, Enabled or Disabled.

Leave All Time
The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

Displaying the GVRP Port Configuration

To display the GVRP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 148 on page 363.

4. In the View GVRP Parameters section, click **View Port Configuration**.

5. Click **View**.

   The GVRP Port Configuration page is shown in Figure 149.

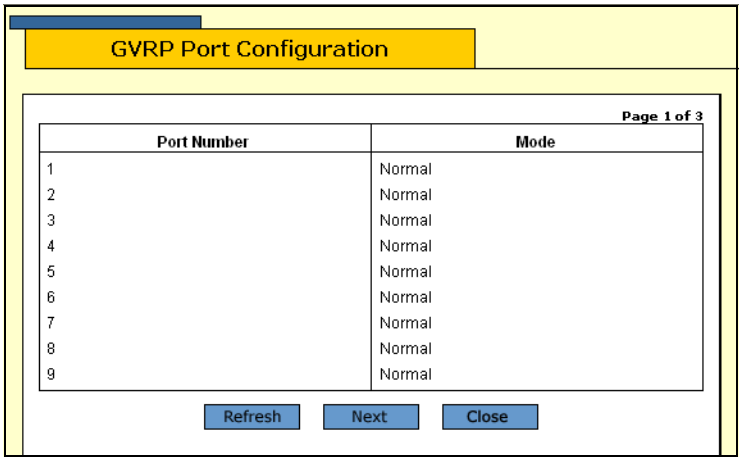

Figure 149. GVRP Port Configuration Page

The GVRP Port Configuration page provides the following information:

Port Number
The port number.

Mode
The port mode, either Normal or None.

Displaying the GVRP Database

To display the GVRP database, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 148 on page 363.

4. In the View GVRP Parameters section, click **View GVRP Database**.

5. Click **View**.

   The GVRP Database page is shown in Figure 150.

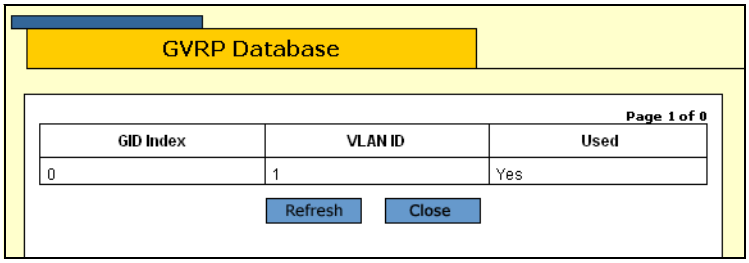

Figure 150. GVRP Database Page

The GVRP Database page provides the following information:

GID Index
The value of the GID index corresponding to the attribute.

VLAN ID
The value of the attribute.

Used
Whether the GID index is currently being used by any port in the GARP application.

Displaying the GVRP State Machine

To display the GVRP state machine, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 148 on page 363.

4. In the View GVRP Parameters section, click **View GVRP State Machine for VLAN** and enter the VLAN number in the box.

5. Click **View**.

   The GVRP State Machine for VLAN page is shown in Figure 151.

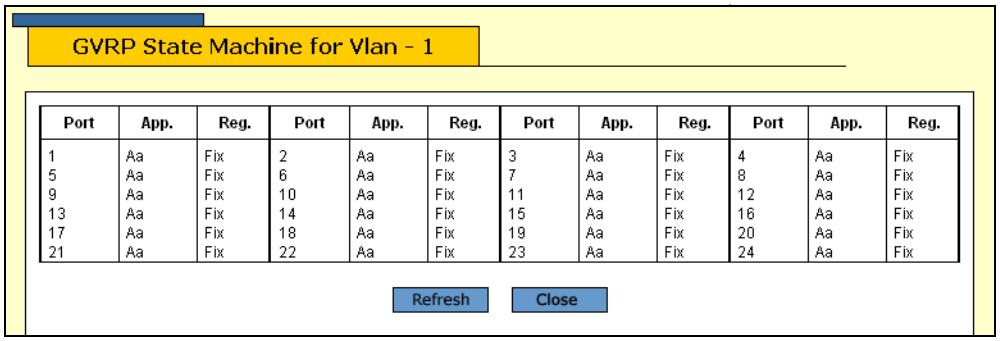
GVRP State Machine for Vlan - 1
Port App. Reg. Port App. Reg. Port App. Reg. Port App. Reg.
1 Aa Fix 2 Aa Fix 3 Aa Fix 4 Aa Fix
5 Aa Fix 6 Aa Fix 7 Aa Fix 8 Aa Fix
9 Aa Fix 10 Aa Fix 11 Aa Fix 12 Aa Fix
13 Aa Fix 14 Aa Fix 15 Aa Fix 16 Aa Fix
17 Aa Fix 18 Aa Fix 19 Aa Fix 20 Aa Fix
21 Aa Fix 22 Aa Fix 23 Aa Fix 24 Aa Fix
Refresh
Close

Figure 151. GVRP State Machine for VLAN Page

The GVRP State Machine for VLAN page provides the information shown in Table 12.

Table 12. GVRP State Machine Parameters

Parameter	Meaning
Port	Port number on the switch; this port belongs to the GARP application. If the GARP application has no ports, "No ports have been assigned" is displayed.

Table 12. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
App	Applicant state machine for the GID index on that particular port. One of:	
	Normal Participant Management state:	
	“Vo”	Very Anxious Observer
	“Ao”	Anxious Observer
	“Qo”	Quiet Observer
	“Lo”	Leaving Observer
	“Vp”	Very Anxious Passive Member
	“Ap”	Anxious Passive Member
	“Qp”	Quiet Passive Member
	“Va”	Very Anxious Active Member
	“Aa”	Anxious Active Member
	“Qa”	Quiet Active Member
	“La”	Leaving Active Member
App (*Continued*)	*Non-Participant Management state:*	
	“Von”	Very Anxious Observer
	“Aon”	Anxious Observer
	“Qon”	Quiet Observer
	“Lon”	Leaving Observer
	“Vpn”	Very Anxious Passive Member
	“Apn”	Anxious Passive Member
	“Qpn”	Quiet Passive Member
	“Van”	Very Anxious Active Member
	“Aan”	Anxious Active Member
	“Qan”	Quiet Active Member
	“Lan”	Leaving Active Member
	The initialized state for the Applicant is Vo.	

Table 12. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
Reg	Registrar state machine for the GID index on that particular port. One of:	
	"Mt"	Empty
	"Lv3"	Leaving substate 3 (final Leaving substate)
	"Lv2"	Leaving substate 2
	"Lv1"	Leaving substate 1
	"Lv"	Leaving substate (initial Leaving substate)
	"In"	In
	"Fix"	Registration Fixed
	"For"	Registration Forbidden
	The initialized state for the Registrar is Mt.	

Displaying the GVRP Counters

To display the GVRP counters, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 148 on page 363.

4. In the View GVRP Parameters section, click **View GVRP Counters**.

5. Click **View**.

   The GVRP Counters page is shown in Figure 152.

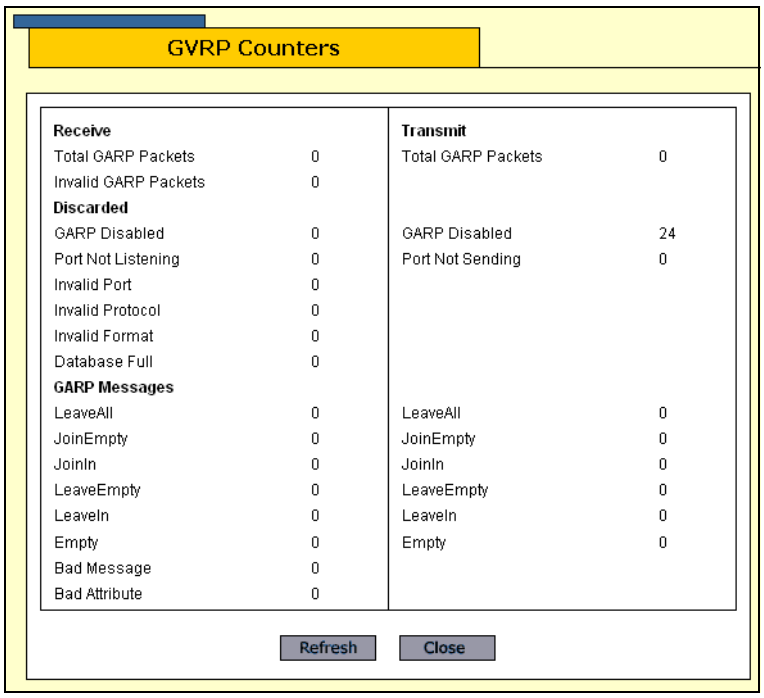

Figure 152. GVRP Counters Page

The GVRP Counters page provides the information shown in Table 13.

Table 13. GVRP Counters

Parameter	Meaning
Receive: Total GARP Packets	Total number of GARP PDUs received by this GARP application.
Transmit: Total GARP Packets	Total number of GARP PDUs transmitted by this GARP application.
Receive: Invalid GARP Packets	Number of invalid GARP PDUs received by this GARP application.
Receive Discarded: GARP Disabled	Number of received GARP PDUs discarded because the GARP application was disabled.
Transmit Discarded: GARP Disabled	Number of GARP PDUs discarded because the GARP application was disabled. This counter is incremented when ports are added to or deleted from the GARP application arising from port movements in the underlying VLAN or STP.
Receive Discarded: Port Not Listening	Number of GARP PDUs discarded because the port that received the PDUs was not listening, that is, MODE=NONE was set on the port.
Transmit Discarded: Port Not Sending	Number of GARP PDUs discarded because the port that the PDUs were to be transmitted on was not sending, that is, MODE=NONE was set on the port.
Receive Discarded: Invalid Port	Number of GARP PDUs discarded because the port that received the PDU does not belong to the GARP application.
Receive Discarded: Invalid Protocol	Number of GARP PDUs discarded because the GARP PDU contained an invalid protocol.
Receive Discarded: Invalid Format	Number of GARP PDUs discarded because the format of the GARP PDU was not recognized.
Receive Discarded: Database Full	Number of GARP PDUs discarded because the database for the GARP application was full, that is, the maximum number of attributes for the GARP application is in use.
Receive GARP Messages: LeaveAll	Number of GARP LeaveAll messages received by the GARP application.
Transmit: GARP Messages: LeaveAll	Number of GARP LeaveAll messages transmitted by the GARP application.

Table 13. GVRP Counters (Continued)

Parameter	Meaning
Receive GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: JoinIn	Total number of GARP JoinIn messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinIn	Total number of GARP JoinIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveIn	Total number of GARP LeaveIn messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveIn	Total number of GARP LeaveIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Empty	Total number of GARP Empty messages received for all attributes in the GARP application.
Transmit GARP Messages: Empty	Total number of GARP Empty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Bad Message	Number of GARP messages that had an invalid Attribute Type value, an invalid Attribute Length value or an invalid Attribute Event value.
Receive GARP Messages: Bad Attribute	Number of GARP messages that had an invalid Attribute Value value.

Displaying the GIP Connected Ports Ring

To display the GIP connected ports ring, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 148 on page 363.

4. In the View GVRP Parameters section, click **View GIP Connected Ports Ring**.

5. Click **View**.

   The GIP Connected Ports Ring page is shown in Figure 153.

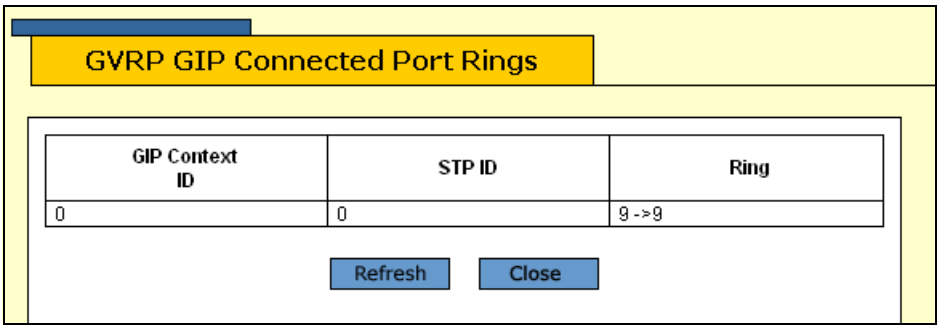

Figure 153. GIP Connected Ports Ring Page

The GIP Connected Ports Ring page displays a table that contains the following columns of information:

GIP Context ID
A number assigned to the instance for the GIP context.

STP ID
Present if the GARP application is GVRP; identifies the spanning tree instance associated with the GIP context.

Ring
The ring of connected ports. Only ports presently in the spanning tree Forwarding state are eligible for membership in the GIP connected

ring. If no ports exist in the GIP connected ring, “No ports are connected” is displayed. If the GARP application has no ports, “No ports have been assigned” is displayed.

Chapter 23

Protected Ports VLANs

This chapter explains how to create, modify, and delete protected ports VLANs and contains the following sections:

- ❒ “Creating a New Protected Ports VLAN” on page 376
- ❒ “Modifying a Protected Ports VLAN” on page 381
- ❒ “Deleting a Protected Ports VLAN” on page 385
- ❒ “Displaying a Protected Ports VLAN” on page 386

Note
For background information on protected ports VLANs, refer to Chapter 28, “Protected Ports VLANs” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a New Protected Ports VLAN

To create a new protected ports VLAN, perform the procedure below:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 123 on page 302.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

   Note
   The Modify and Remove buttons are not included in the tab if the only VLAN on the switch is the Default_VLAN.

   This tab displays the VLANs in a table that contains the following columns of information:

   VLAN ID
   The VID number assigned to the VLAN.

   (Client) Name
   The name of the VLAN.

   Uplink Port
   This column is applicable only when the switch is operating in one of the two multiple VLAN modes. The column lists the port that is functioning as the uplink port for the other ports on the switch.

   Type
   This column contains “Port Based” for both port-based and tagged VLANs, “GVRP Dynamic” for VLANs created by GVRP, and “Protected” for protected ports VLANs.

   Protocol
   Not used.

   Tagged(T)/Untagged(U) Port
   Lists the ports of the VLAN. Tagged ports are designated with a “T” and untagged ports with a “U.”

4. To create a new protected ports VLAN, click **Add**.

The Add New VLAN page is shown in Figure 154.

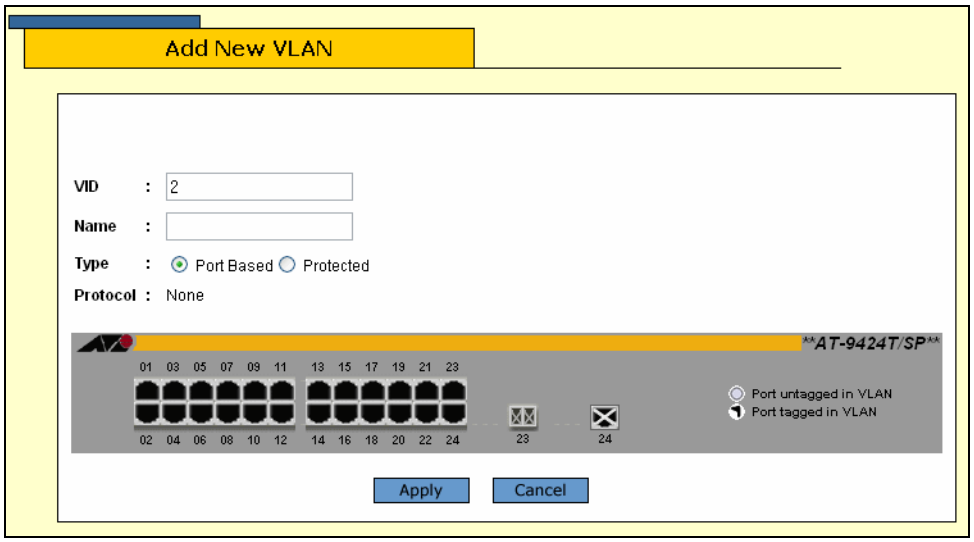

Figure 154. Add New VLAN Page

5. Select the **VID** field and enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

   The switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-9400 Series switch to a network that already contains VLANs that use VIDs 2 through 24, the AT-S63 software will still use VID 2 as the default value when you create the first VLAN on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

   Note
   A VLAN must have a VID.

6. Select the **Name** field and enter a name for the new VLAN.

   The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

   Note
   A VLAN must be assigned a name.

7. Select **Protected** as the Type.
8. Select the ports for the protected ports VLAN by clicking the ports in the switch image. (Designating group membership of the ports is performed later in the procedure.)

   Clicking repeatedly on a port toggles the port through the following possible settings:

   Untagged port

   Tagged port

   Port is not a member of the VLAN

9. Click **Apply**.

Note
Any untagged ports you assign to the new VLAN are automatically removed from their current untagged VLAN assignment.

The Add New Protected VLAN page is shown in Figure 155.

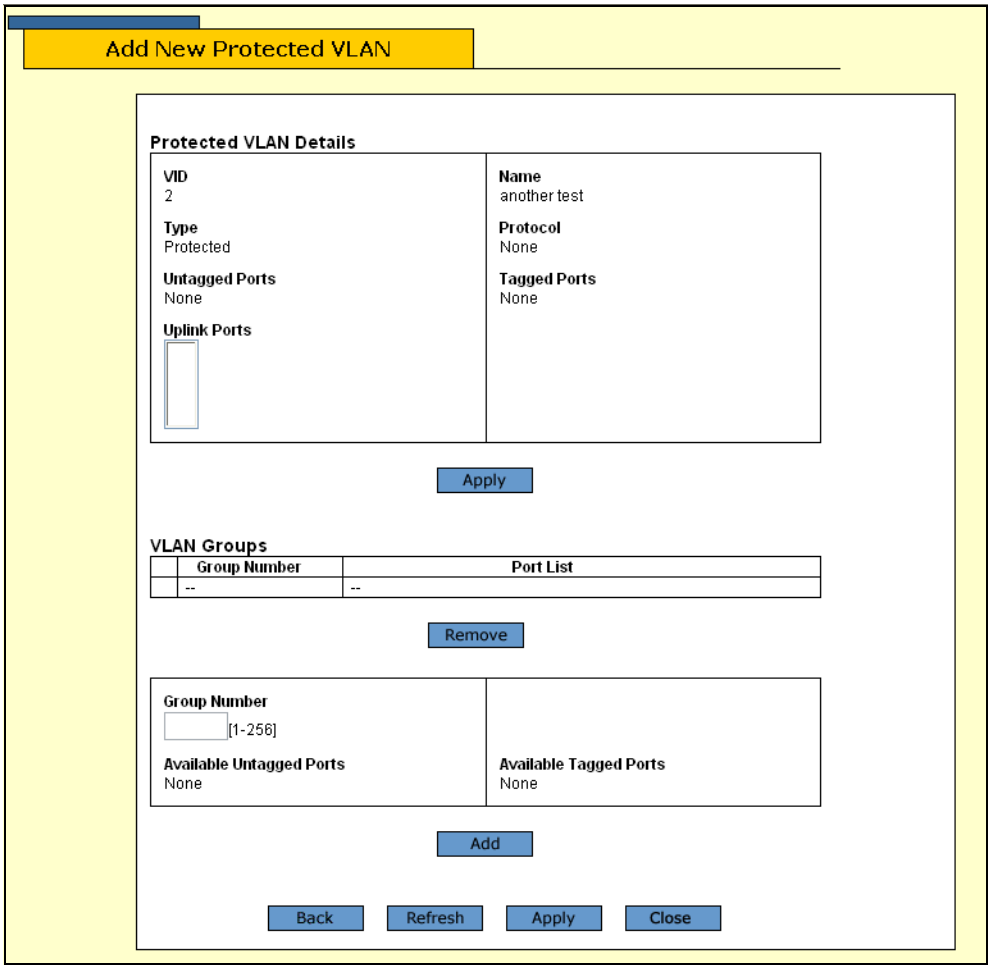

Figure 155. Add New Protected VLAN Page

10. Use the Uplinks Port menu to select an uplink port for the groups of this protected ports VLAN.

    The menu lists all of the ports you selected as members of this VLAN. You can select more than one uplink port. To select multiple ports, hold down the Ctrl key when selecting the ports.

11. Click **Apply**.

12. In the Group Number field, enter a group number for one of the groups you want to create in the VLAN. Each group on the switch must be given a unique group number. The range is 1 to 256.

13. In the Available Untagged Port and Available Tagged Ports lists, select the port you want to be in the group. You can assign more than one port to group. To select multiple ports from a list, use <Ctrl>+click.

14. Click **Add**.

The switch creates the group and adds it to the VLAN Groups section of the window.

15. Repeat steps 12 to 14 to create the other groups for the VLAN.
16. After you have assigned all of the ports in the VLAN to a group, click the **Apply** button at the bottom of the window.

    The management software will not allow you to create the VLAN until all of the ports have been assigned to a group.

    The new protected ports VLAN is now ready for network operations.
17. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Protected Ports VLAN

This procedure explains how to change the uplink port of a protected ports VLAN and how to add or remove ports from a VLAN. When modifying a protected ports VLAN, note the following:

- You cannot change the VID of a protected port VLAN.
- You cannot change the name of a VLAN from a web browser management session; but you can from a local or Telnet session.
- If you are adding untagged ports, the ports must be untagged members of the Default_VLAN or a port-based or tagged VLAN. They cannot be members of another protected ports VLAN.
- An untagged port removed from a VLAN is automatically returned to the Default_VLAN.
- Changing the uplink port of a protected ports VLAN will require recreating all the VLAN's groups. If you need to change the uplink port, Allied Telesyn recommends that you write down on paper the VLAN's current configuration (i.e., port to group assignments). This information will make it easier for you to recreate the current configuration, with whatever modifications you want to make, when you perform the procedure. To display a VLAN's configuration, refer to "Displaying a Protected Ports VLAN" on page 386.

To modify a protected ports VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 123 on page 302.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

4. Click the button next to the name of the protected ports VLAN you want to modify.

5. Click **Modify**.

   The Modify VLAN window for the VLAN is displayed.

6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:

Untagged port

Tagged port

Port is not a member of the VLAN

7. After making the necessary changes, click **Apply**.

Note
Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN will leave the port as an untagged member of no VLAN.

The Modify Protected VLAN page is shown in Figure 156.

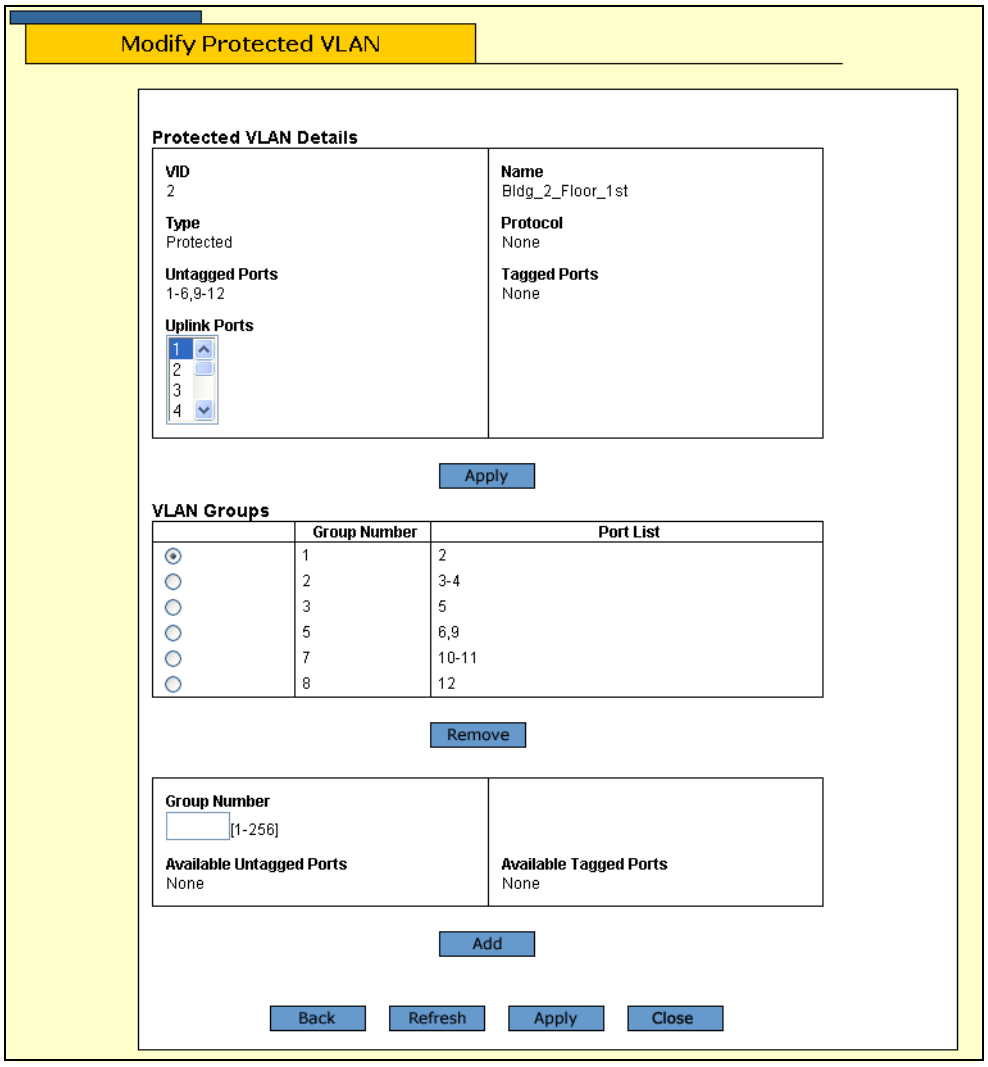

Figure 156. Modify Protected VLAN Page

8. To change the uplink port, do the following:

Note
Changing the uplink port will delete all the groups.

   a. Use the Uplinks Port menu to select a new uplink port for the groups of this protected ports VLAN. The menu lists all of the ports you selected as members of this VLAN. You can select more than one uplink port. To select multiple ports, hold down the Ctrl key when selecting the ports.

   b. When the confirmation prompt is displayed, click **OK**.

   c. Click **Apply**.

d. Recreate the groups.

9. To delete a group, do the following:

   a. Click the circle next to the group number and click **Remove**. The ports of the deleted group are now listed in the Available Untagged Ports and Available Untagged Ports lists.

   b. Assign the ports to another group or use the ports to create a new group. All the ports in a protected ports VLAN must belong to a group.

10. To modify an existing group, such as to add or remove ports, you must first delete the group and then recreate it with the desired changes.

> **Note**
> To completely remove a port from a protected ports VLAN, you must deselect the port in the graphical image of the switch in step 6, then delete its group, and finally recreate the group without the port.

11. To create a new group, do the following:

    a. In the Group Number field, enter a group number for the new group. Each group on the switch must be given a unique group number. The range is 1 to 256.

    b. In the Available Untagged Port and Available Tagged Ports lists, select the port to be in the group. You can assign more than one port to group. To select multiple ports from a list, hold down the Ctrl key when selecting the ports.

    c. Click **Add**. The switch creates the group and adds it to the VLAN Groups section of the window.

12. After you have made the necessary changes and assigned all of the ports to a group, click **Apply** at the bottom of the window.

    VLAN changes are immediately implemented on the switch.

13. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Protected Ports VLAN

To delete a protected ports VLAN from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 123 on page 302.

3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 143 on page 346.

4. Click the button next to the name of the protected ports VLAN you want to delete. You cannot delete the Default_VLAN.

5. Click **Remove**.

   A confirmation prompt is displayed.

6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

   If you click OK, the VLAN is deleted from the switch. All ports in the VLAN are returned to the Default_VLAN as untagged ports.

7. To permanently save the change, select the **Save Config** menu selection.

Displaying a Protected Ports VLAN

To display the details of a protected port VLAN, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Layer 2** option.

3. The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 123 on page 302.

4. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 145 on page 355.

5. Click the circle next to the protected ports VLAN you want to view and click **View**.

   The View Protected VLAN page is shown in Figure 157.

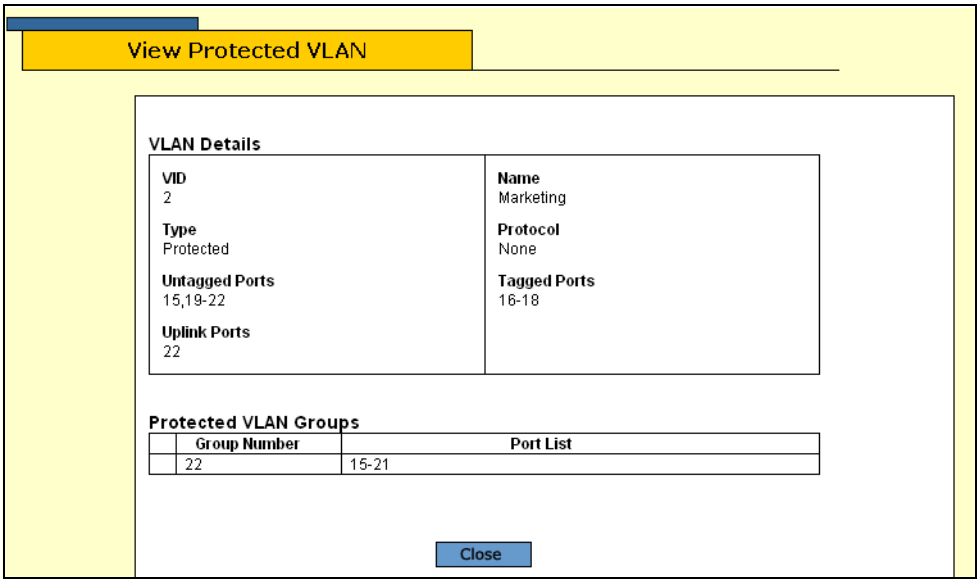

Figure 157. View Protected VLAN Page

The VLAN Details section displays the following information.

VID
The VLAN ID.

Type
The VLAN type which is always Protected.

Untagged Ports
The untagged ports that are members of the VLAN.

Uplink Ports
The uplink port(s) for this group of ports.

Name
The VLAN name.

Protocol
Not use.

Tagged Ports
The tagged ports that are members of the VLAN.

The Protected VLAN Groups section displays the following information:

Group Number
The number assigned to the group.

Port List
The ports that are members of this group.

6. Click **Clear** to close the page.

Section VI

Port Security

The chapters in this section provide the procedures for configuring port security. The chapters include:

- Chapter 24, “MAC Address-based Port Security” on page 391
- Chapter 25, “802.1x Port-based Network Access Control” on page 397

Chapter 24

MAC Address-based Port Security

This chapter explains how to configure and display the MAC address security levels on the ports on the switch. It contains the following sections:

- "Configuring Port Security" on page 392
- "Displaying the Port Security Level" on page 395

Note
For background information on port security, refer to Chapter 30, "MAC Address-based Port Security," in the *AT-S63 Management Software Menus Interface User's Guide*.

Configuring Port Security

To configure security for the ports, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 158.

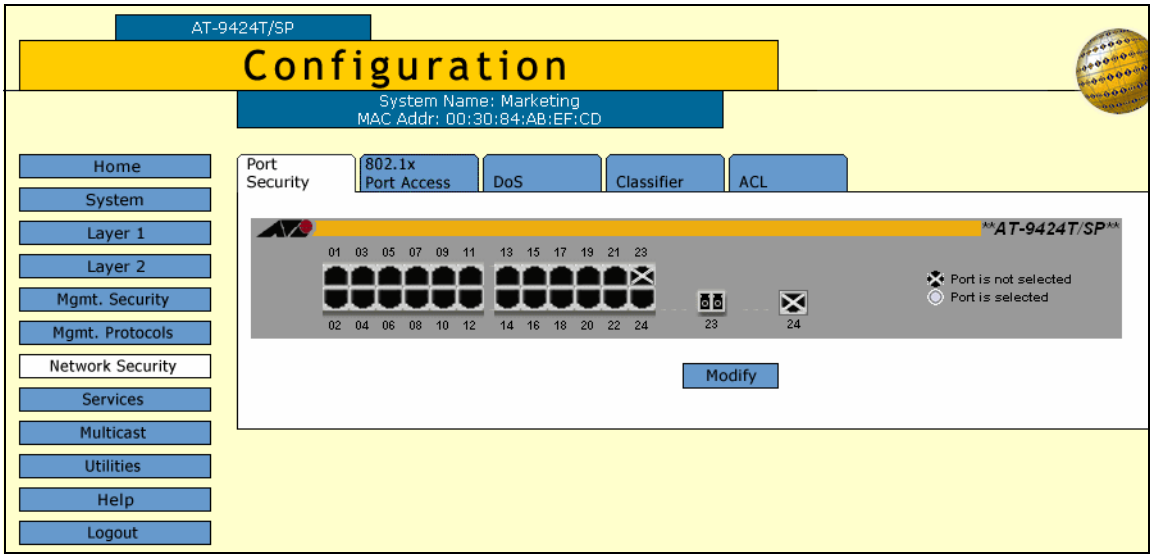

Figure 158. Port Security Tab (Configuration)

3. In the graphical image of the switch, click the ports you want to configure and click **Modify**. The Security for Ports page is shown in Figure 161.

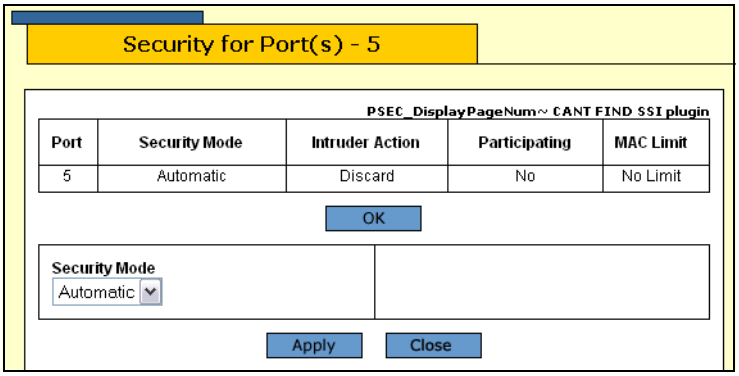

Figure 159. Security for Ports Page (Configuration)

4. From the Security Mode pull-down menu, select the desired port security level for the port. Options are:

   Automatic
   Disables port security on a port. This is the default setting.

   Limited
   Allows you to specify a maximum number of dynamic source MAC addresses a port can learn. Once a port has learned its maximum number, it will not learn any new addresses and will only accept frames from the source nodes of the learned addresses.

   A dynamic MAC address learned on a port operating in the Limited security mode never times out from the MAC address table, even when the corresponding end node is inactive.

   You can add static addresses to a port running this security level. Static addresses are not included in the count of the maximum number of dynamic addresses.

   Secured
   Instructs a port to forward frames using only static MAC address. The port will not learn any dynamic MAC addresses and will delete any dynamic addressees that it has already learned. Only those end nodes whose MAC addresses are entered as static addresses can forward frames through the port.

   Locked
   Instructs a port to immediately stop learning new dynamic MAC addresses. Frames are forwarded using the dynamic MAC addresses that the port has already learned and any static MAC addresses assigned to the port.

   Dynamic MAC addresses learned by the port prior to the activation of this security level never time out from the MAC address table, even when the corresponding end nodes are inactive. However, the port will not learn any new dynamic addresses.

   You can continue to add new static MAC addresses to a port operating under this security level.

5. If you select the Limited security level, additional options are displayed in the window for you to configure. They are defined here:

   Intrusion Action
   Specifies what the switch should do if a port receives an invalid frame. Options are

   - ❒ Discard - Discards the invalid frame.
   - ❒ Trap - Discards the invalid frame and sends an SNMP trap.
   - ❒ Discard - Discards the invalid frame, sends an SNMP trap, and disables the port.

Threshold
Specifies the maximum number of dynamic MAC addresses you want the port to be able to learn. The range is 1 to 256. The default is 100.

Port Participating
Applies only when the intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard. If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send the SNMP trap or disable the port. If you want the switch to send a trap and/or disable the port, you must sent this option to Yes.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port Security Level

To display the MAC address security level of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Network Security**.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 160.

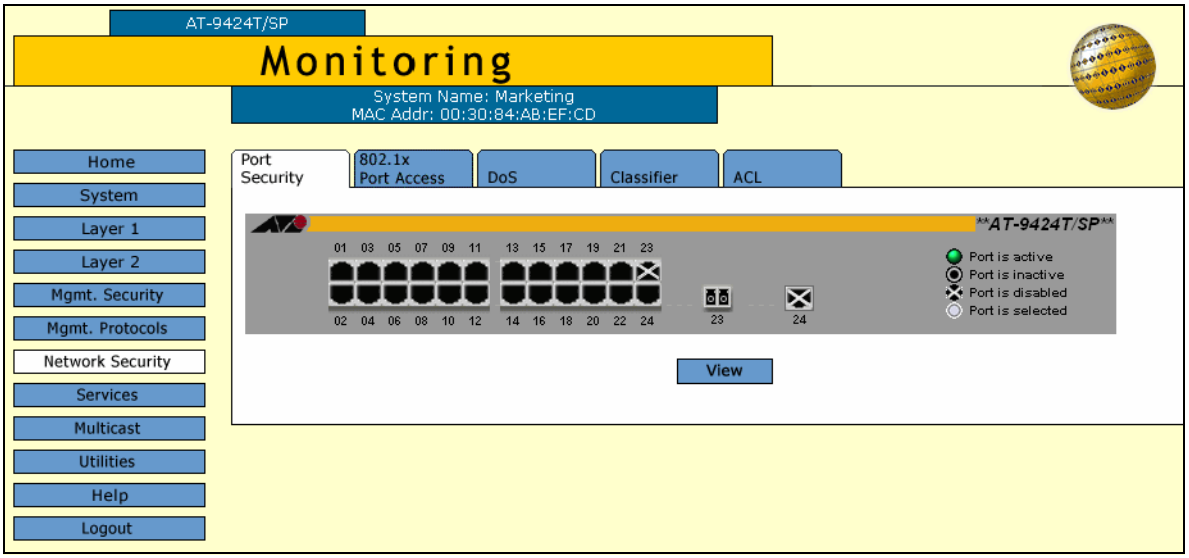

Figure 160. Port Security Tab (Monitoring)

3. Click the port whose port security level you want to view. A selected port turns white. You can select more than one port at a time.

4. Click **View**.

The Security for Port(s) page is shown in Figure 161.

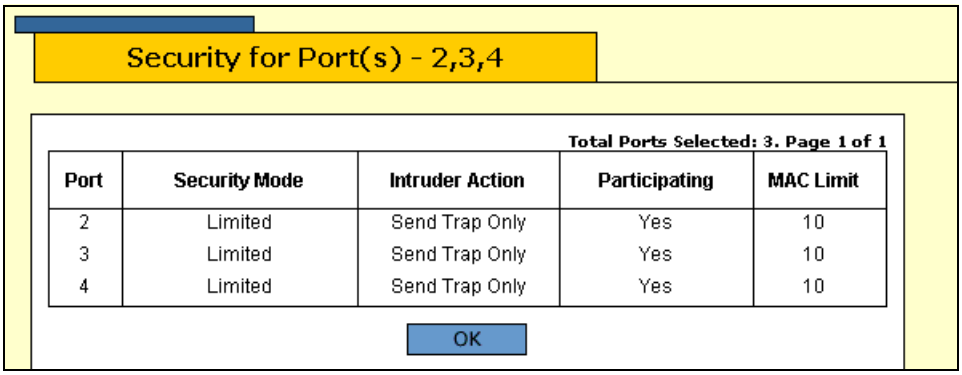

Figure 161. Security for Port(s) Page

The Security for Ports page displays a table that contains the following columns of information:

Port
The number of the port.

Security Mode
The active security mode on the port. The possible settings are Automatic, Limited, Secured, and Locked.

Intruder Action
The column specifies the action taken by the switch if a port receives an invalid packet. The possible settings are:

Discard - The port discards invalid packets. This is the default.

Trap - The port discards invalid packets and sends a trap. This action applies only to the Limited security mode.

Trap/Disable - The port discards invalid packets, sends a trap, and disables the port. This action applies only to the Limited security mode.

Participating
This column applies only when the intrusion action for a port is set to trap or disable. This option does not apply when intrusion action is set to No Action (discard). If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send a trap or disable the port.

MAC Limit
This column specifies the maximum number of dynamic MAC addresses the port learns. It only applies when a port is operating in the Limited security mode.

Chapter 25

802.1x Port-based Network Access Control

This chapter contains instructions on how to configure the 802.1x Port-based Network Access Control feature on the switch. The chapter contains the following sections:

- ❒ “Setting Port Roles” on page 398
- ❒ “Enabling or Disabling 802.1x Port-based Network Access Control” on page 400
- ❒ “Configuring Authenticator Port Parameters” on page 401
- ❒ “Configuring Supplicant Port Parameters” on page 405
- ❒ “Displaying the Port-based Network Access Control Parameters” on page 407
- ❒ “RADIUS Accounting” on page 411

Note
For background information on port-based network access control, refer to Chapter 31, “802.1x Port-based Network Access Control,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Setting Port Roles

To set port roles for port-based network access control, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 162.

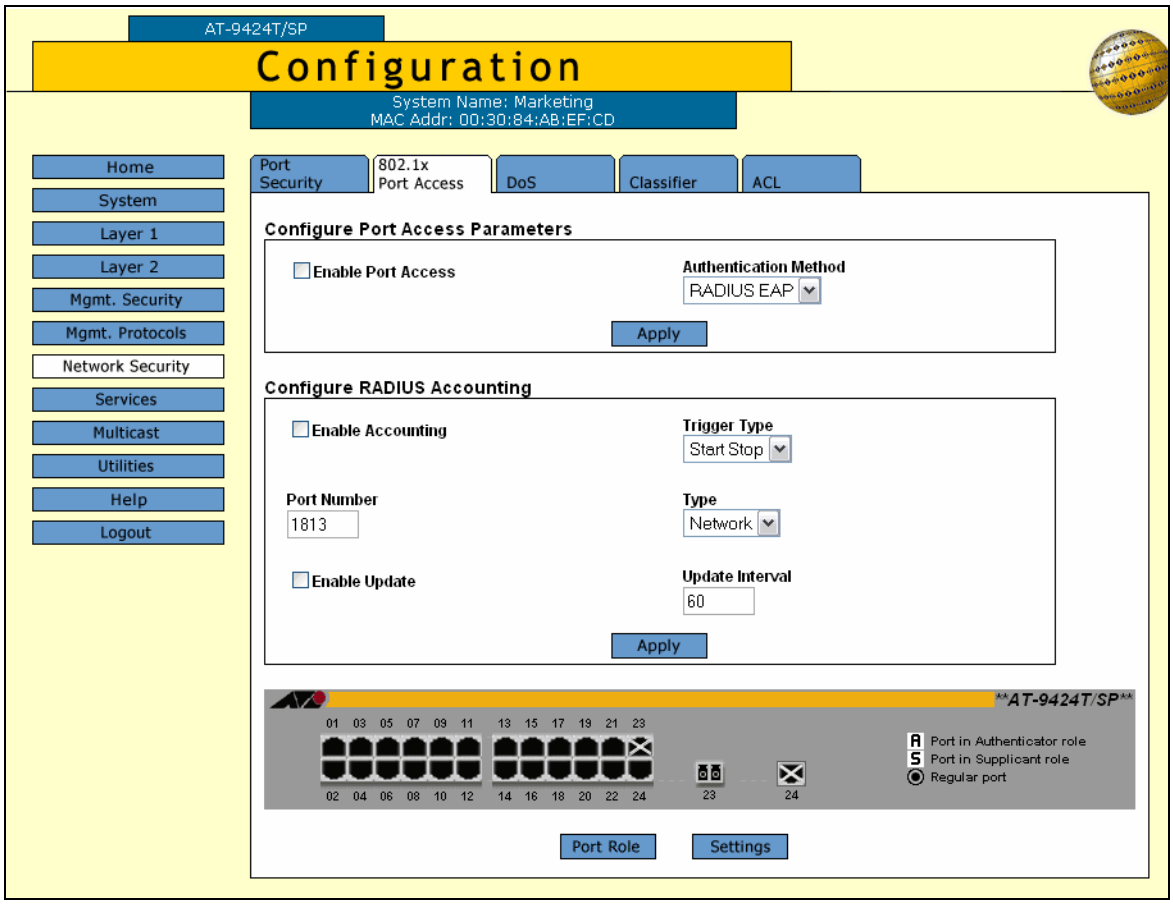

Figure 162. 802.1x Port Access Tab (Configuration)

The graphical image of the switch shows which ports have already been assigned port roles. An "A" indicates that a port is functioning as an authenticator while an "S" indicates the port is functioning as a supplicant. A black port has not been assigned a port role and is not participating in port-based access control. This is the default setting for a port.

4. To set a port's role, click on the port. The selected port turns white. You can select more than one port at a time.

5. Click **Port Role**.

   The Port Role Configuration page is shown in Figure 163.

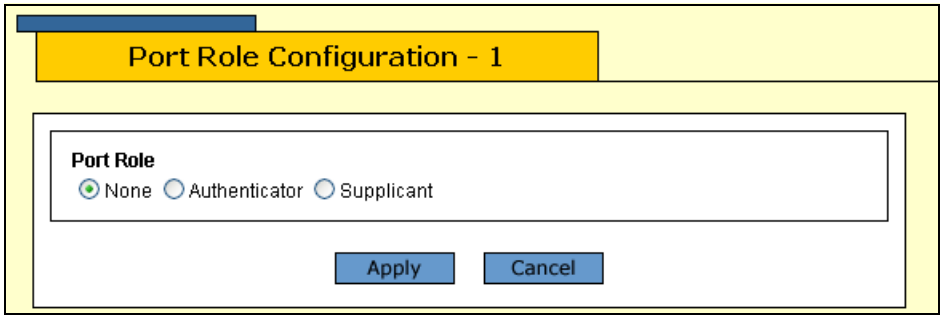

Figure 163. Port Role Configuration Page

6. Select the desired role for the port. A port can have only one port role at a time. The possible settings are:

   None
   The port is not to participate in port-based access control. This is the default setting.

   Authenticator
   The port is to function as an authenticator. This is the appropriate setting if the port is connected to a supplicant.

   Supplicant
   The port is to function as an supplicant. This is the appropriate setting if the port is connected to an authenticator.

7. Click **Apply**.

   The new role is immediately implemented on the port.

   To enable or disable port-based access control, go to "Enabling or Disabling 802.1x Port-based Network Access Control" on page 400. Then, to configure authenticator port settings, go to "Configuring Authenticator Port Parameters" on page 401. To configure supplicant port settings, go to "Configuring Supplicant Port Parameters" on page 405.

Enabling or Disabling 802.1x Port-based Network Access Control

To enable or disable 802.1x Port-based Network Access Control, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 162 on page 398.

4. Click the **Enable Port Access** check box. A check in the box means that the feature is activated on the switch. No check means that the feature is disabled.

   For instructions on configuring the accounting feature, refer to “RADIUS Accounting” on page 411.

5. Click **Apply**.

   A change to the status of 802.1x Port-based Network Access Control is immediately implemented on the switch.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring Authenticator Port Parameters

To configure authenticator port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **802.1x Port Access** tab. The 802.1x Port Access tab is shown in Figure 162 on page 398.

4. Click the authenticator port that you want to configure. You can select more that one authenticator port at a time. The selected port turns white.

   Note
   The role of a port must be set to authenticator before you can configure the authenticator port settings. For instructions on how to set a port's role, refer to "Setting Port Roles" on page 398.

5. Click **Settings**.

The Authenticator Parameters page is shown in Figure 164.

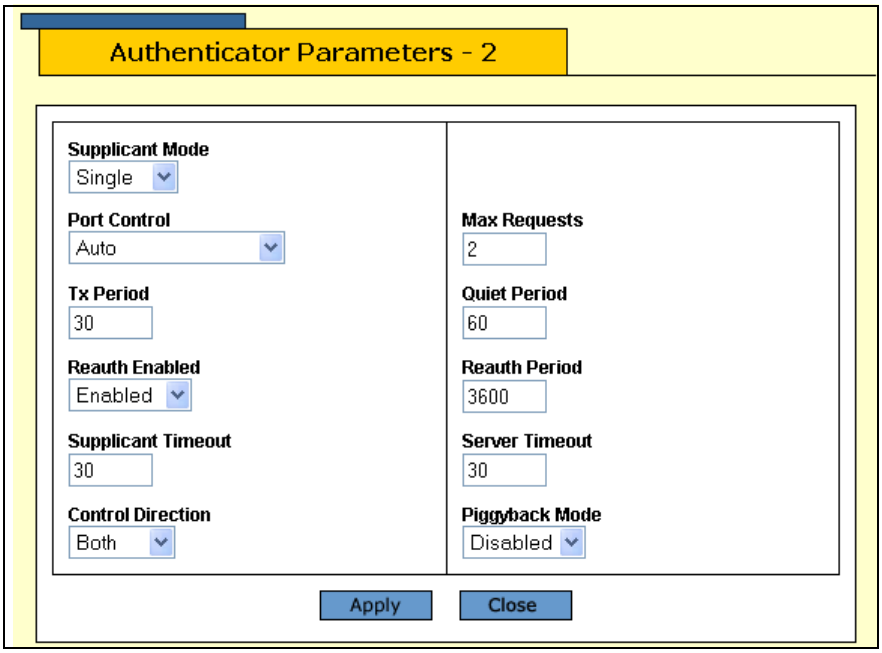

Figure 164. Authenticator Parameters Page

6. Configure the following parameters as necessary:

Supplicant Mode
This parameter sets the supplicant mode of an authenticator port and can take the following values:

- **Single**: Configures the port to accept only one authentication. This authenticator mode should be used together with the piggy-back mode. When an authenticator port is set to the Single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port.
- **Multiple**: Configures the port to accept up to 20 authentications. Every client using an authenticator port in this mode must have a username and password combination.

Port Control
The possible settings are:

Auto - Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication messages between the client

and the authentication server. Each client that attempts to access the network is uniquely identified by the switch using the client's MAC address. This is the default setting.

Force-authorized - Disables IEEE 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client.

Force-unauthorized **-** Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface

Max Requests
Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

TX Period
Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

Quiet Period
Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

Reauth Enabled
Controls whether the client must periodically reauthenticate. The default setting of enabled requires the client to periodically reauthenticate. The time period between reauthentications is set with the Reauth Period option. If this parameter is set to disabled, the client is not required to reauthenticate after the initial authentication, unless there is a change to the status of the link between the supplicant and the switch or the switch is reset or power cycled. The options are Enabled or Disabled. The default is Enabled.

Reauth Period
Enables periodic reauthentication of the client, which is disabled by default. The Reauth Enabled option must be set to Enabled for this parameter to be operational. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Supplicant Timeout
Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Server Timeout
Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 seconds.

Control Direction
Specifies how the port handles ingress and egress broadcast and multicast packets when in the unauthorized state. When a port is set to the Authenticator role, it remains in the unauthorized state until the client logs on by providing a username and password combination. In the unauthorized state, the port only accepts EAP packets from the client. All other ingress packets that the port might receive from the client, including multicast and broadcast traffic, are discarded until the supplicant has logged in. The options are:

Ingress - A port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client, but forwards all egress broadcast and multicast traffic to the same client.

Both - A port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the client until the client logs in. This is the default.

Piggyback Mode
Controls who can use the switch port in cases where there are multiple clients (e.g., the port is connected to an Ethernet hub). If set to enabled, the port allows all clients on the port to piggy-back onto the initial client's authentication. The port forwards all packets, regardless of the client, after one client has been authenticated. If set to Disabled, the switch port forwards only those packets from the client who was authenticated and discards packets from all other users.

7. Click **Apply**.

   Changes to the authenticator settings are immediately implemented on a port.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring Supplicant Port Parameters

To configure supplicant port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 162 on page 398.

4. Click the supplicant port that you want to configure. You can select more that one supplicant port at a time. The selected port turns white.

   Note
   A port must already be designated as a supplicant before you can configure its settings. For instructions on how to set the role of a port, refer to "Setting Port Roles" on page 398.

5. Click **Settings**.

   The Supplicant Parameters page is shown in Figure 164.

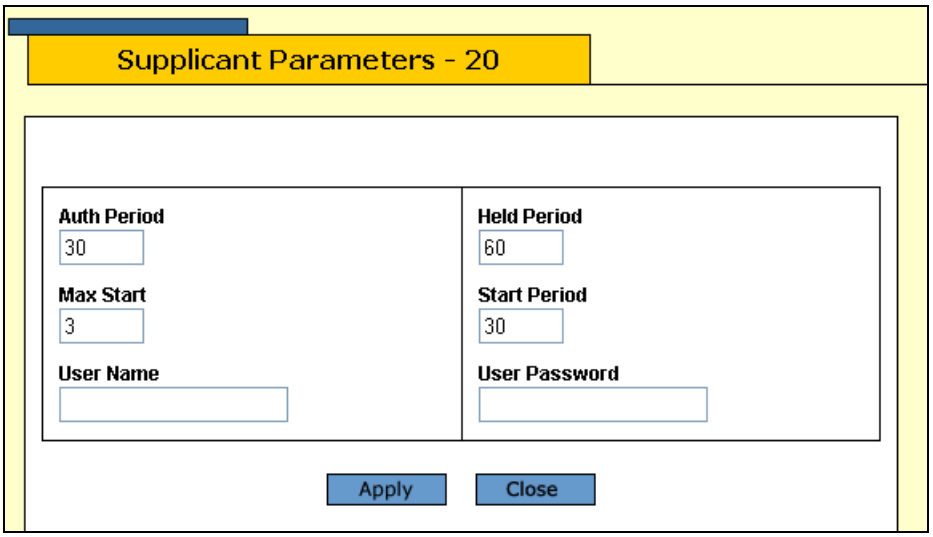

Figure 165. Supplicant Parameters Page

6. Configure the following parameters as needed:

   Auth Period
   Specifies the period of time in seconds that the supplicant waits for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 60 seconds. The default is 30 seconds.

   Held Period
   Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535 seconds. The default value is 60 seconds.

   Max Start
   Specifies the maximum number of times the supplicant sends EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

   Start Period
   Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.

   User Name
   Specifies the username for the switch port. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case sensitive.

   User Password
   Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case sensitive.

7. Click **Apply**.

   Changes to the supplicant settings are immediately implemented on a port.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port-based Network Access Control Parameters

You can display information about the port-based network access control status and settings of the ports on the switch. This section contains the following procedures:

- ”Displaying the Port Status” (next)
- “Displaying the Port Settings” on page 408

Displaying the Port Status

To display the port-based network access control port status, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Network Security**.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 160 on page 395.

3. Select the **802.1x Port Access** tab. The 802.1x Port Access tab is shown in Figure 166.

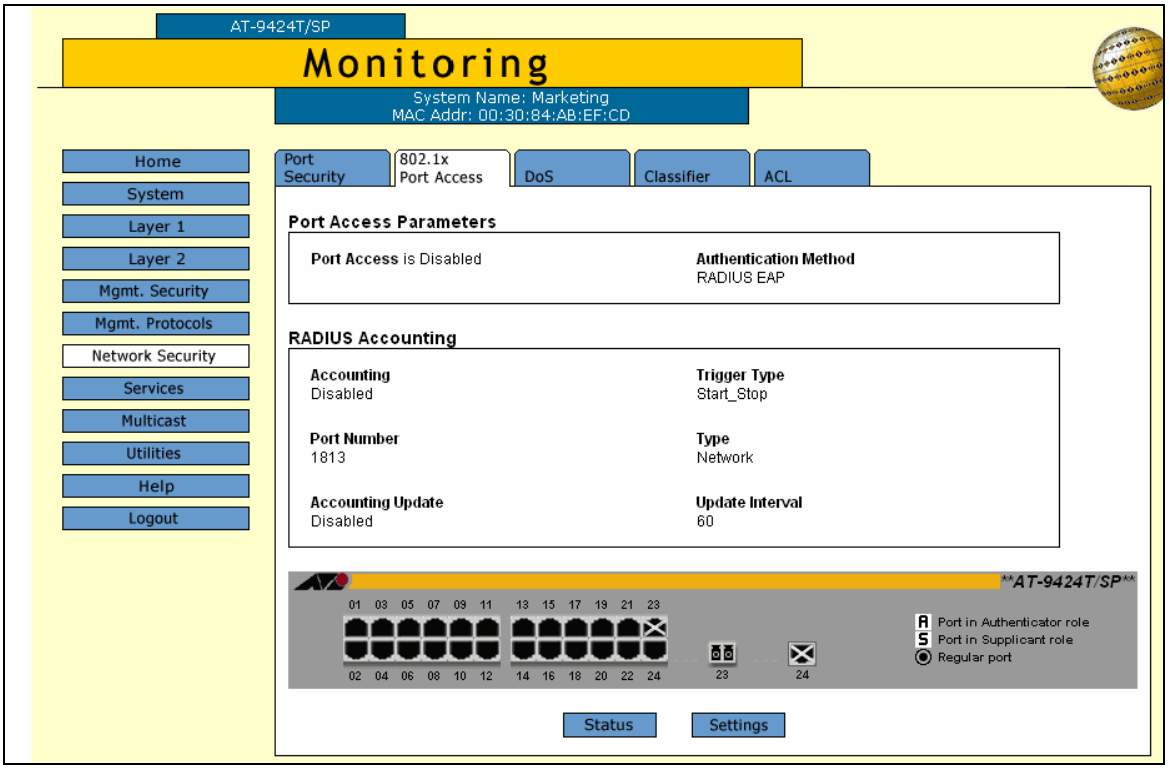

Figure 166. 802.1x Port Access Tab (Monitoring)

4. To see the status of the port, click the port and click **Status**. You can select more than one port at a time.

   The Port Access Port Status page is shown in Figure 167.

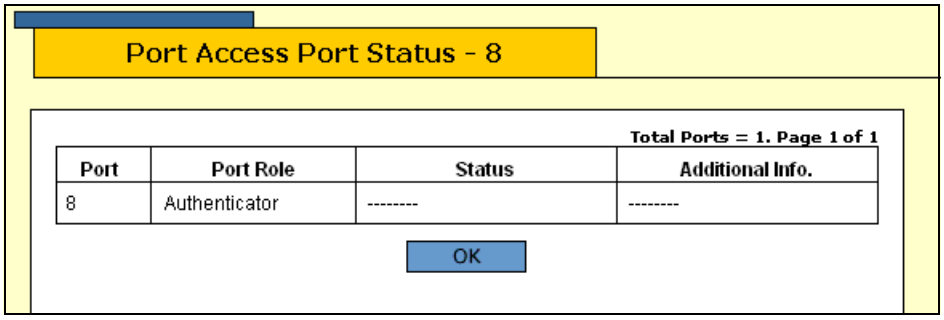

Figure 167. Port Access Port Status Page

The Port Access Port Status page displays a table that contains the following columns of information:

Port
The port number.

Port Role
The port role: None, Authenticator, or Supplicant.

Status
The options include: Initialize, Disconnected, and so forth.

Additional Info.
More information about the port including the MAC address.

Displaying the Port Settings

To display the port-based network access control port settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select **Network Security**.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 160 on page 395.

3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 166 on page 407.

4. To review the port access settings, click OK to close the Port Access Port Status page and return to the 802.1x Port Access tab

5. To see the port settings, click the port and click **Settings**. You can select more than one port at a time.

> **Note**
> To view the settings of multiple ports, you must select ports that have the same port role (authenticator or supplicant).

For authenticator port(s), the Authenticator Port Parameters page is displayed, as shown in Figure 168.

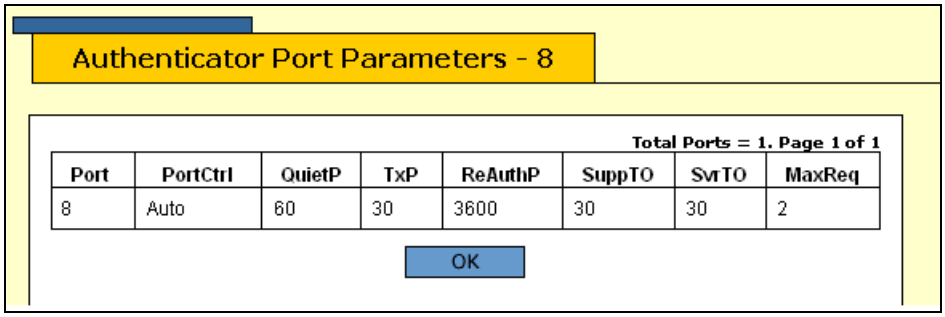

Figure 168. Authenticator Port Parameters Page

The Authenticator Port Parameters page displays a table that contains the following columns of information:

Port
The port number.

PortCtrl
The port control setting. The possible settings are:

Force-authorized - 802.1x port-based authentication is disabled.

Force-unauthorized - The port is in an unauthorized state, ignoring attempts by the client to authenticate.

Auto - 802.1x port-based authentication is enabled.

QuietP
The number of seconds the port remains in a quiet state following a failed authentication exchange with the client.

TxP
The number of seconds that the switch waits for a response to an EAP Request packet/identity packet from the client before retransmitting the request.

ReAuthP
The frequency of the periodic reauthentication of the client.

SuppTO
The switch-to-client retransmission time for the EAP Request packet.

MaxReq
The maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session.

For supplicant port(s), the Supplicant Port Parameters Page is displayed, as shown in Figure 169.

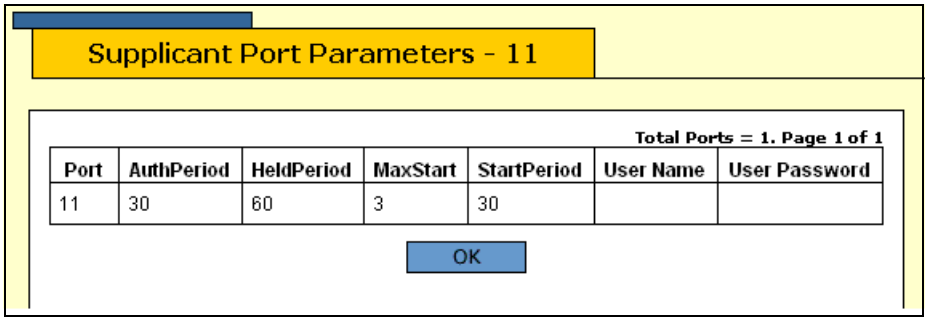

Figure 169. Supplicant Port Parameters Page

The Supplicant Port Parameters page displays a table that contains the following columns of information:

Port
The port number.

AuthPeriod
The period of time in seconds that the supplicant waits for a reply from the authenticator.

HeldPeriod
The amount of time the supplicant is to refrain from trying to recontact the authenticator in the event that the end user provides an invalid user name and/or password.

MaxStart
The maximum number of times the supplicant sends EAPoL-Start packets before assuming that there is no authenticator present.

StartPeriod
The time period between successive attempts by the supplicant to establish contact with an authenticator when there is no reply.

User Name
The user name for the port.

User Password
The password for the port.

RADIUS Accounting

The AT-S63 management software supports RADIUS accounting for ports operating in the Authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. For background information on this feature, refer to Chapter 31, "802.1x Port-based Network Access Control" in the *AT-S63 Management Software Menus Interface User's Guide*. This feature is disabled by default on the switch.

Configuring RADIUS Accounting

To configure RADIUS accounting, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 158 on page 392.

3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 162 on page 398

4. In the Configure RADIUS Accounting section, configure the following parameters as necessary.

   Enable Accounting
   This parameter activates or deactivates RADIUS accounting on the switch. Select Enabled to activate the feature or Disabled to deactivate it. The default is Disabled.

   Trigger Type
   This parameter specifies the action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

   Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

   Stop - The switch sends accounting information only when a client logs off.

   Port Number
   Specifies the UDP port for RADIUS accounting. The default is port 1813.

Type
This parameter specifies the type of RADIUS accounting. The default is Network. You cannot change this value.

Enable Update
This parameter controls whether the switch is to send interim accounting updates to the RADIUS server. A check in the box indicates that updating is enabled. No check in the box means that updating is disabled.

Update Interval
Specifies the intervals at which the switch sends interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

5. Click **Apply**.

   Changes to the accounting settings are immediately implemented on the switch.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the RADIUS Accounting Settings

To display the RADIUS accounting settings, perform the following procedure:

1. From the home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Network Security** option.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 160 on page 395.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 170.

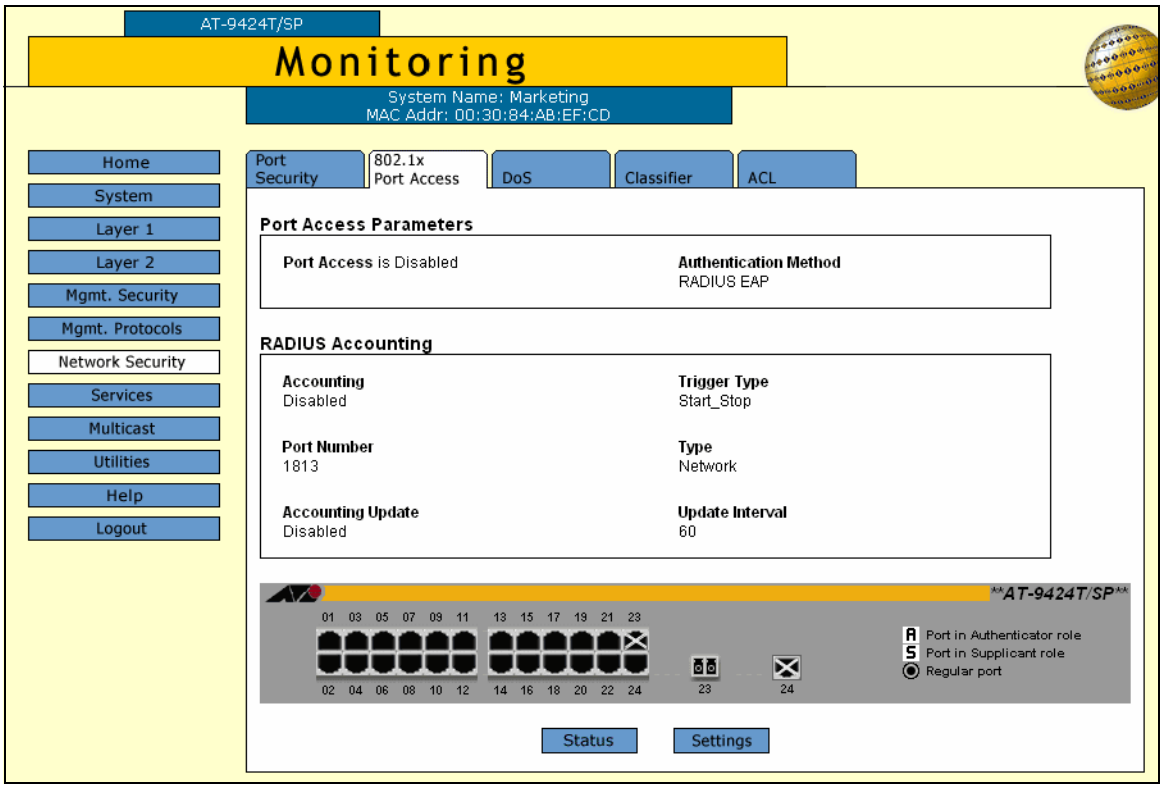

Figure 170. 802.1x Port Access Tab (Monitoring)

The RADIUS Accounting section provides the following information:

Accounting
The status of RADIUS accounting, either Enabled or Disabled.

Trigger Type
The action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

Stop - The switch sends accounting information only when a client logs off.

Port Number
The UDP port for RADIUS accounting.

Type
The type of RADIUS accounting. The default is Network.

Accounting Update
Whether or not the switch sends interim accounting updates to the RADIUS server. The options are Enabled or Disabled.

Update Interval
The intervals, in seconds, at which the switch sends interim accounting updates to the RADIUS server.

The graphical image of the switch and the Status and Settings buttons refer to the 802.1x Port-based Network Access Control settings, described in “Displaying the Port-based Network Access Control Parameters” on page 407.

Section VII

Management Security

The chapters in this section contain the procedure for implementing management security on the switch to prevent unauthorized changes to a switch's parameter settings. The chapters include:

- ❒ Chapter 26, "Encryption Keys, PKI, and SSL" on page 417
- ❒ Chapter 27, "Secure Shell (SSH)" on page 425
- ❒ Chapter 28, "TACACS+ and RADIUS Protocols" on page 431
- ❒ Chapter 29, "Management Access Control List" on page 443

Chapter 26

Encryption Keys, PKI, and SSL

This chapter explains how to view the encryption keys, PKI-based certificates, and SSL settings and includes the following sections:

- ❒ “Displaying the Encryption Keys” on page 418
- ❒ “Displaying the PKI Settings and Certificates” on page 420
- ❒ “Displaying the SSL Settings” on page 423

Note
To configure encryption keys, PKI, or SSL, you must use the AT-S63 menus or CLI interface.

For information about encryption keys, refer to Chapter 33, “Encryption Keys,” in the *AT-S63 Management Software Menus Interface User’s Guide.*

For information about PKI and SSL, refer to Chapter 34, “PKI Certificates and SSL” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Displaying the Encryption Keys

To configure the encryption keys, you must use the AT-S63 menus or command line interface. For more information about encryption keys, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the encryption keys, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Mgmt. Security** option.

   The Mgmt. Security page is displayed with the Mgmt. ACL tab displayed by default, as shown in Figure 184 on page 449.

3. Select the **Keys** tab.

   The Keys tab is shown in Figure 171.

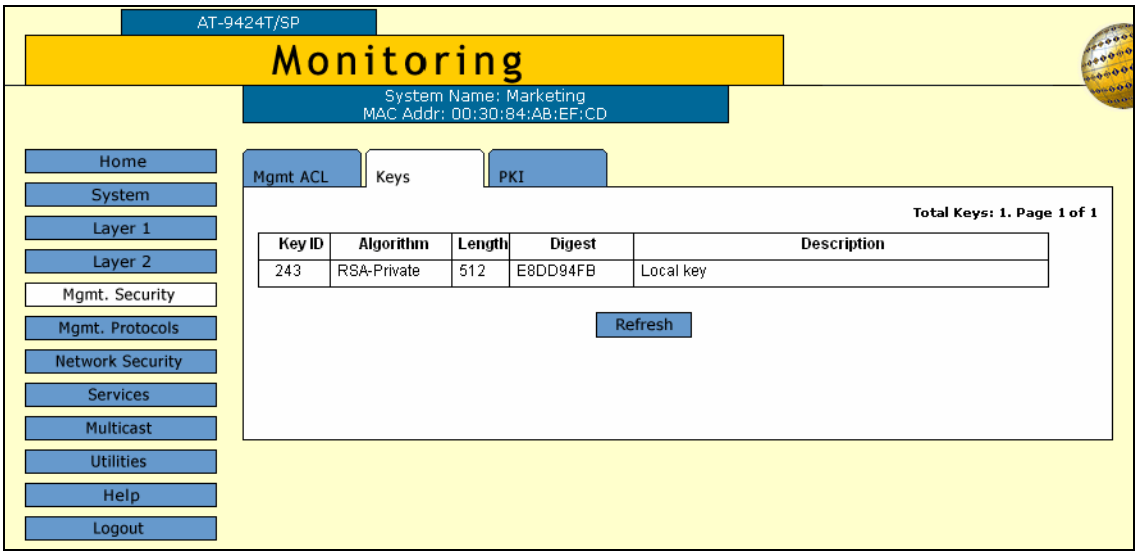

Figure 171. Keys Tab (Monitoring)

The Keys tab displays a table that contains the following columns of information:

ID
The identification number of the key.

Algorithm
The algorithm used in creating the encryption. This is always RSA - Private.

Length
The length of the key in bits.

Digest
The CRC32 value of the MD5 digest of the public key.

Description
The key's description.

You use these keys when you configure Secure Sockets Layer (SSL) or Secure Shell (SSH). To configure SSL you must use the AT-S63 menus or CLI interface. To configure SSH, refer to Chapter 27, "Secure Shell (SSH)" on page 425.

Displaying the PKI Settings and Certificates

You can view the current PKI settings and certificates on the switch. To configure the PKI settings and certificates, you must use the AT-S63 menus or command line interface. For more information about PKI, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the PKI settings and certificates, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Mgmt. Security** option.

   The Mgmt. Security page is displayed with the Mgmt. ACL tab displayed by default, as shown in Figure 184 on page 449.

3. Select the **PKI** tab.

   The PKI tab is shown in Figure 172.

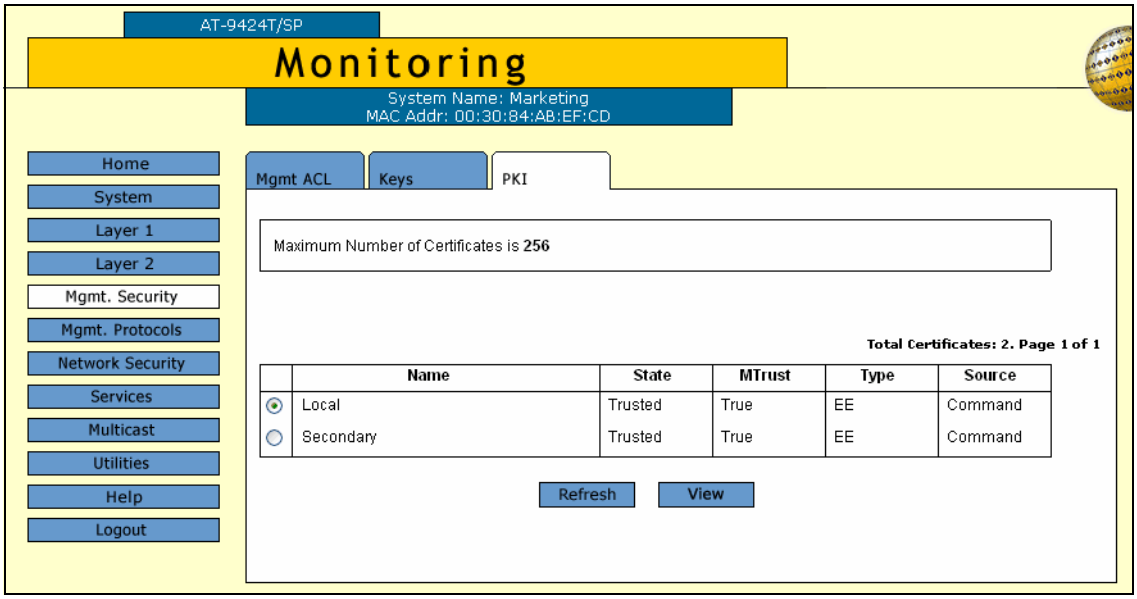

Figure 172. PKI Tab (Monitoring)

The upper section states the maximum number of certificates that can be configured on the switch.

The lower section displays a table that lists the currently configured certificates and contains the following columns of information:

Name
The certificate name.

State
The state of the certificate, one of the following:

Trusted - The certificate is from a trusted CA.

Untrusted - The certificate is from an untrusted CA.

MTrust (Manually Trusted)
The certificate has been manually verified that it is from a trusted or untrusted authority.

Type
The certificate type, one of the following:

EE - The certificate was issued by a CA.

CA - The certificate belongs to a CA.

Self - A self-signed certificate.

Source
The certificate was created on the switch.

4. To view the details about a certificate, click the certificate and click **View**.

   The X509 Certificate Details page is shown in Figure 173.

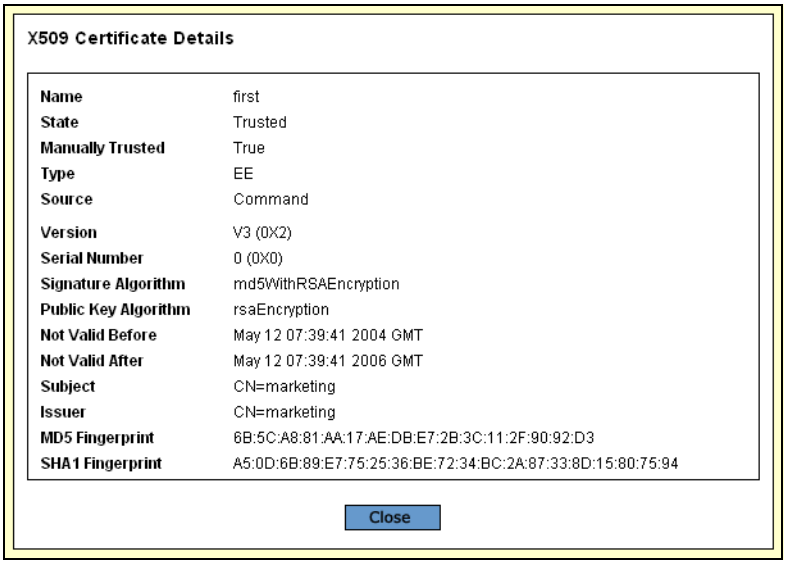

Figure 173. X509 Certificate Details Page

The X509 Certificate Details page provides the following information about the certificate:

Name
The name of the certificate.

State
Whether the certificate is Trusted or Untrusted.

Manually Trusted
You verified the certificate is from a trusted or untrusted authority.

Type
The type of the certificate. The options are EE, SELF, and CA.

Source
The certificate was created on the switch.

Version
The version number of the AT-S63 management software.

Serial Number
The certificate's serial number.

Signature Algorithm
The signature algorithm of the certificate.

Public Key Algorithm
The public key algorithm.

Not Valid Before
The date the certificate became active.

Not Valid After
The date the certificate expires. Self-signed certificates are valid for two years.

Subject
The Subject distinguished name.

Issuer
The certificate issuer's distinguished name.

MD5 Fingerprint
The MD5 algorithm. This value provides a unique sequence for each certificate consisting of 16 bytes.

SHA1 Fingerprint
The Secure Hash Algorithm. This value provides a unique sequence for each certificate consisting of 20 bytes.

5. Click **Close** to close the page.

Displaying the SSL Settings

To configure the SSL settings, you must use the AT-S63 menus or command line interface. For information, refer to the *AT-S63 Management Software Menus Interface User's Guide* and the *AT-S63 Management Software Command Line Interface User's Guide*.

To display the SSL settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 179 on page 436.

3. Select the **SSL** tab.

   The SSL tab is shown in Figure 171.

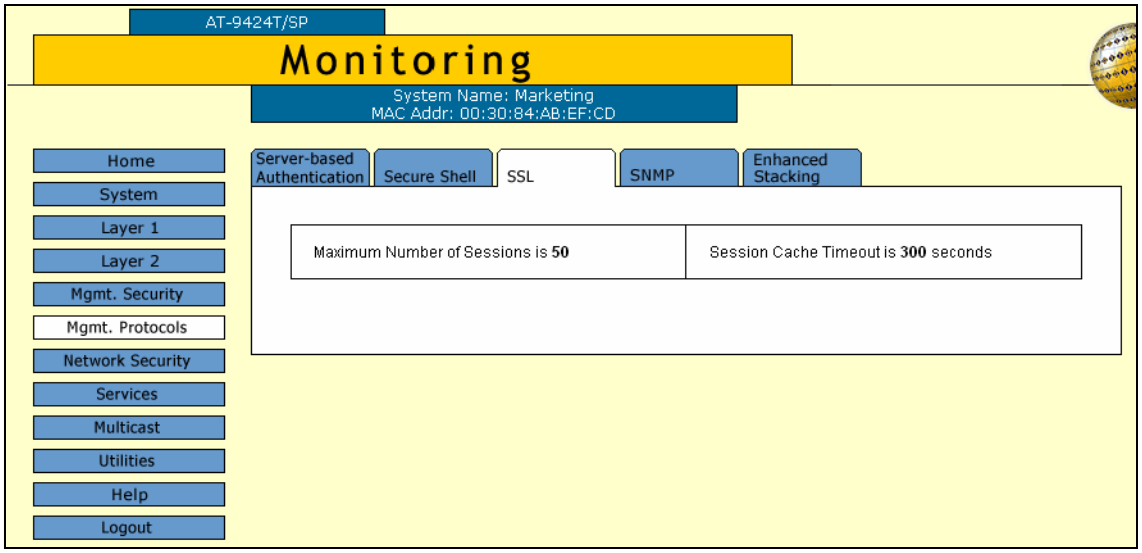

Figure 174. SSL Tab (Monitoring)

The SSL tab provides the following information:

Maximum Number of Sessions
The maximum number of SSL sessions allowed at one time.

Session Cache Timeout
The length of time before the session cache times out, in seconds.

Chapter 27

Secure Shell (SSH)

This chapter explains how to configure the Secure Shell (SSH) protocol and contains the following sections:

- ❒ “Configuring SSH” on page 426
- ❒ “Displaying the SSH Settings” on page 428

Note
For background information on SSH, refer to Chapter 35, “Secure Shell (SSH),” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring SSH

To configure SSH, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177 on page 432.

3. Select the **Secure Shell** tab.

   The Secure Shell tab is shown in Figure 175.

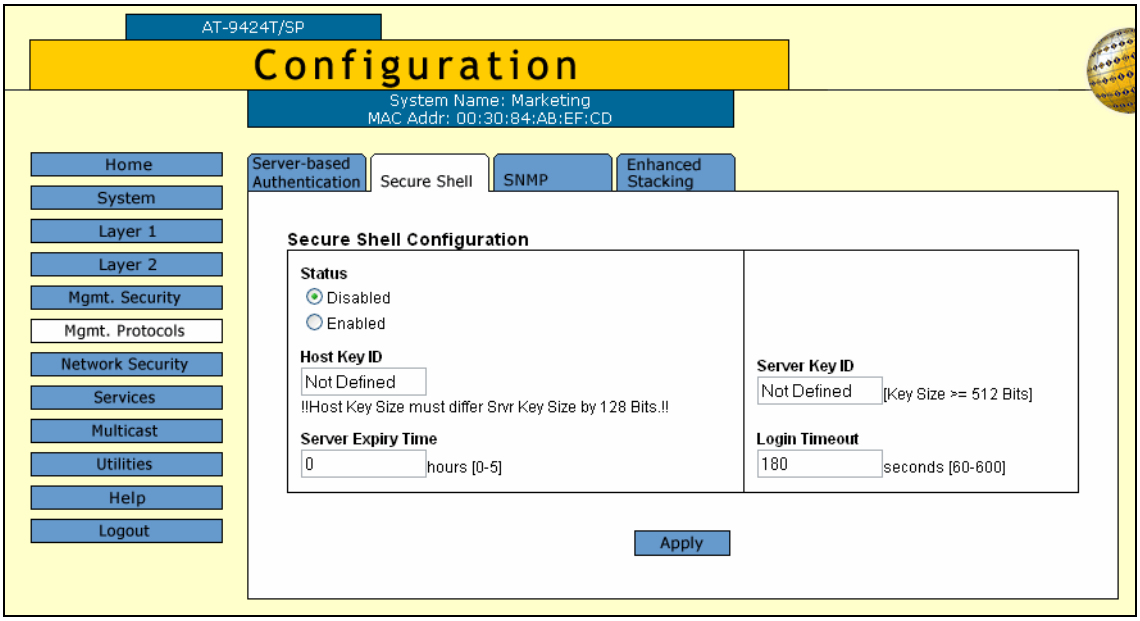

Figure 175. Secure Shell Tab (Configuration)

4. Configure the following parameters as necessary:

   Status
   Enable the SSH server after you have finished the configuration. Or, click Disabled while you are configuring the protocol. SSH must be disabled while you are configuring the protocol. This is the default.

Note
You cannot disable the SSH server when there is an active SSH connection.

Host Key ID
Enter the ID number of the encryption key for the SSH host. The key must already exist on the switch. To view key ID numbers, refer to "Displaying the Encryption Keys" on page 418. The default is Not Defined.

Note
You cannot create encryption keys from the web browser interface, but you can from the menus and command line interfaces.

Server Key ID
Enter the ID number of the encryption key for the SSH server. The key must already exist on the switch. The default is Not Defined.

Server Expiry Time
Set the time, in hours, for the server key to expire.

This timer determines how often the server key is regenerated. A server key is regenerated for security purposes. A server key is only valid for the time period configured in the Server Key Expiry (Expiration) Time timer. Allied Telesyn recommends that you set this field to 1. With this setting, a new key is generated every hour.

Login Timeout
Enter a number between 60 and 600. The default is 180.

This is the time it takes to release the SSH server from an incomplete SSH client connection. Enter a time in seconds. The default is 180 seconds (3 minutes). The range is 60 to 600 seconds.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the SSH Settings

To view the Secure Shell settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 179 on page 436.

3. Select the **Secure Shell** tab.

   The Secure Shell tab is shown in Figure 176.

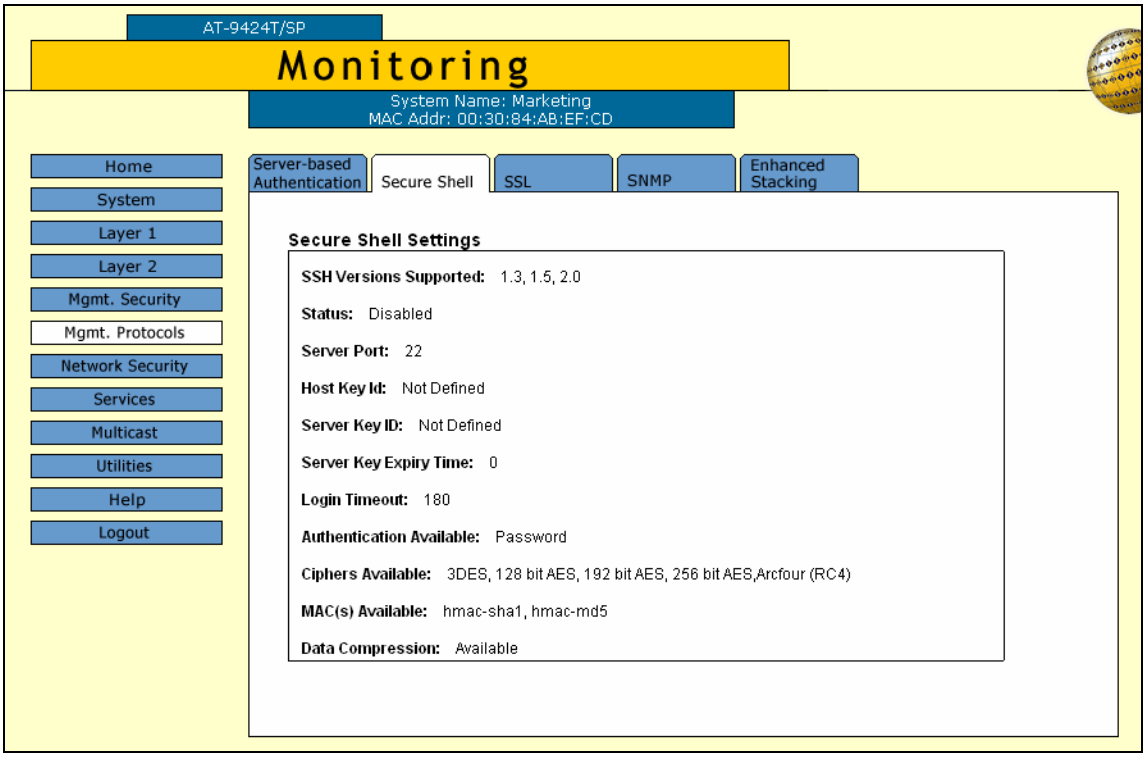

Figure 176. Secure Shell Tab (Monitoring)

The Secure Shell tab provides the following information:

SSH Versions Supported
The versions of SSH that the AT-S63 management software supports.

Status
Whether or not the SSH server is enabled or disabled.

Server Port
The well-known port for SSH. The default is port 22.

Host Key ID
The host key ID defined for SSH.

Server Key ID
Server key ID defined for SSH.

Server Key Expiry Time
Length of time, in hours, until the server key is regenerated. The default is 0 hours which means the server key is not regenerated.

Login Timeout
Time, in seconds, until a SSH server is released from an incomplete connection with a SSH client.

Authentication Available
Authentication method available. Currently, password authentication is the only supported method.

Ciphers Available
SSH ciphers that are available on the switch.

MAC(s) Available
Message Authorization Code (MAC) that is used to validate incoming SSH messages to the server. Two algorithms are supported.

Data Compression
Whether or not data compression is available on the switch. Data compression is useful for networks that have a slow throughput speed.

Chapter 28

TACACS+ and RADIUS Protocols

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedures:

- ❒ “Enabling or Disabling TACACS+ or RADIUS” on page 432
- ❒ “Configuring TACACS+” on page 434
- ❒ “Displaying the TACACS+ Settings” on page 436
- ❒ “Configuring RADIUS” on page 438
- ❒ “Displaying the RADIUS Settings” on page 440

Note
For background information on the authentication protocols, refer to Chapter 36, “TACACS+ and RADIUS Protocols,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Enabling or Disabling TACACS+ or RADIUS

To enable or disable server-based authentication, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 177.

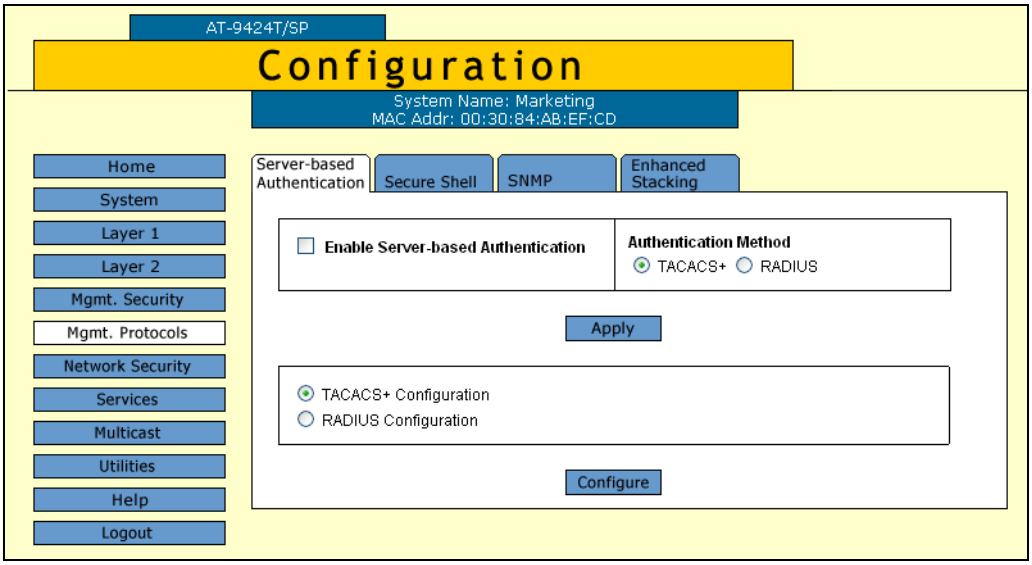

Figure 177. Server-based Authentication Tab (Configuration)

3. To select an authentication protocol, in the Authentication Method section of the tab, click either RADIUS or TACACS+. The default is TACACS+.

   Note
   The switch can support only one authentication protocol at a time. Additionally, you cannot select a different authenticator protocol when this feature is enabled.

4. To enable or disable the authentication feature on the switch, click the Enable Server-based Authentication check box. A check in the box indicates that this feature is enabled. No check indicate the feature is disabled. The default is disabled.

Note
The Enable Server-based Authentication check box applies only when you are using the TACACS+ or RADIUS client software to support new manager accounts. If you will be using RADIUS for 802.1x port-based access control only and not for new manager accounts, you should leave the check box empty. The switch will still be able to access the RADIUS configuration information for 802.1x port-based access control.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

   To configure TACACS+, go to "Configuring TACACS+" on page 434.
   To configure RADIUS, go to "Configuring RADIUS" on page 438.

Configuring TACACS+

To configure TACACS+, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38

2. Select the **Server-based Authentication** tab.

   The Server-based Authentication tab is shown in Figure 177 on page 432.

3. In lower section of the Server-based Authentication tab, click TACACS+ Configuration and click **Configure**.

   The TACACS+ Client Configuration page is shown in Figure 178.

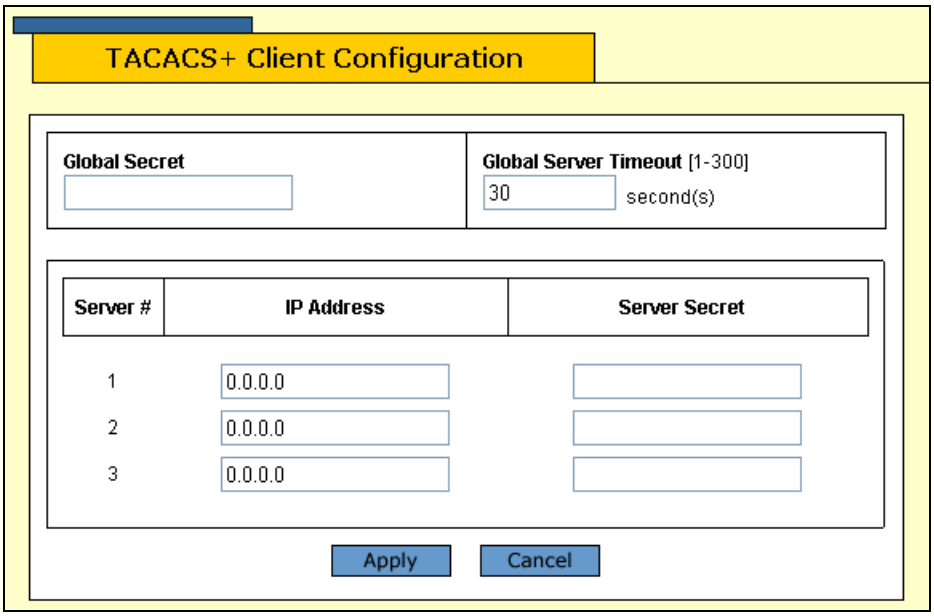

Figure 178. TACACS+ Client Configuration Page

4. Configure the following parameters as necessary.

   Global Secret
   If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

   Global Server Timeout
   This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server

cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there are no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and **Encryption Key**
Use these fields to specify the IP addresses and encryption secrets of up to three network servers containing TACACS+ server software. You can leave an encryption field blank if you entered the server's secret in the Global Secret field.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the TACACS+ Settings

To display the TACACS+ settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. Select the **Mgmt. Protocols** option.

   The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 179.

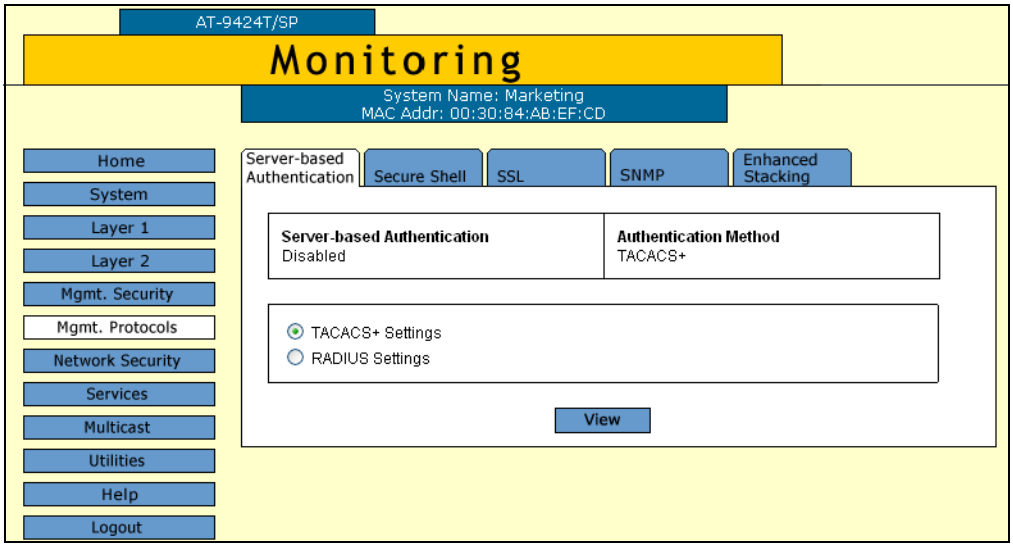

Figure 179. Server-Based Authentication Tab (Monitoring)

   The upper part of the page shows if server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view either the settings for the current authentication method.

3. In the lower portion of the tab, click TACACS+ Settings.

4. Click **View**.

The TACACS+ client configuration page is shown in Figure 180.

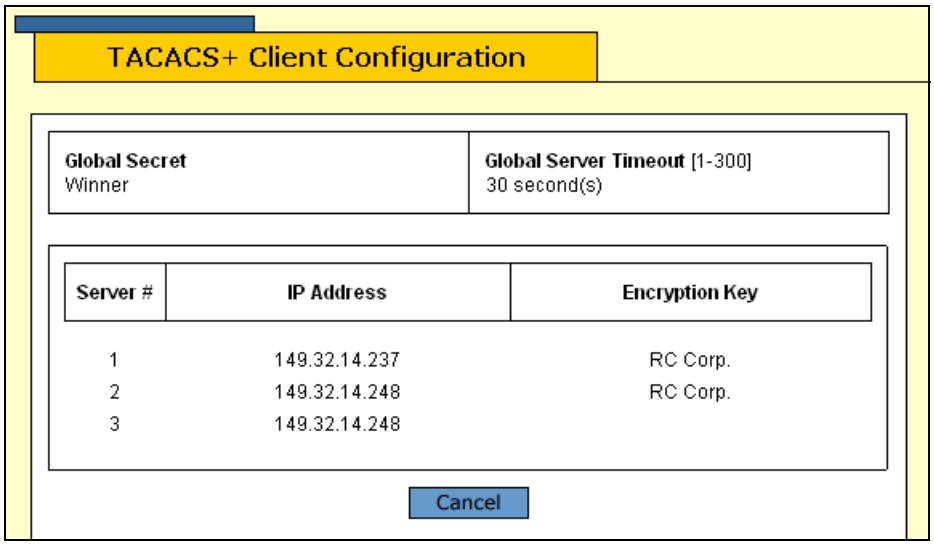

Figure 180. TACACS+ Client Configuration Page

The upper portion of the page provides the following information:

Global Secret
The TACACS+ server encryption secret.

Global Server Timeout
The maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond.

The lower portion of the page displays a table that contains the following columns of information:

Server #
The server number, one of three.

IP Address
IP addresses of up a network server containing TACACS+ server software.

Encryption Key
Encryption key for the server. This parameter is blank if all the TACACS+ servers have the same encryption secret.

Configuring RADIUS

To configure RADIUS, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38

2. Select the **Server-based Authentication** tab.

   The Server-based Authentication tab is shown in Figure 177 on page 432.

3. In lower section of the Server-based Authentication tab, click RADIUS Configuration and click **Configure**.

   The RADIUS Client Configuration page is shown in Figure 178.

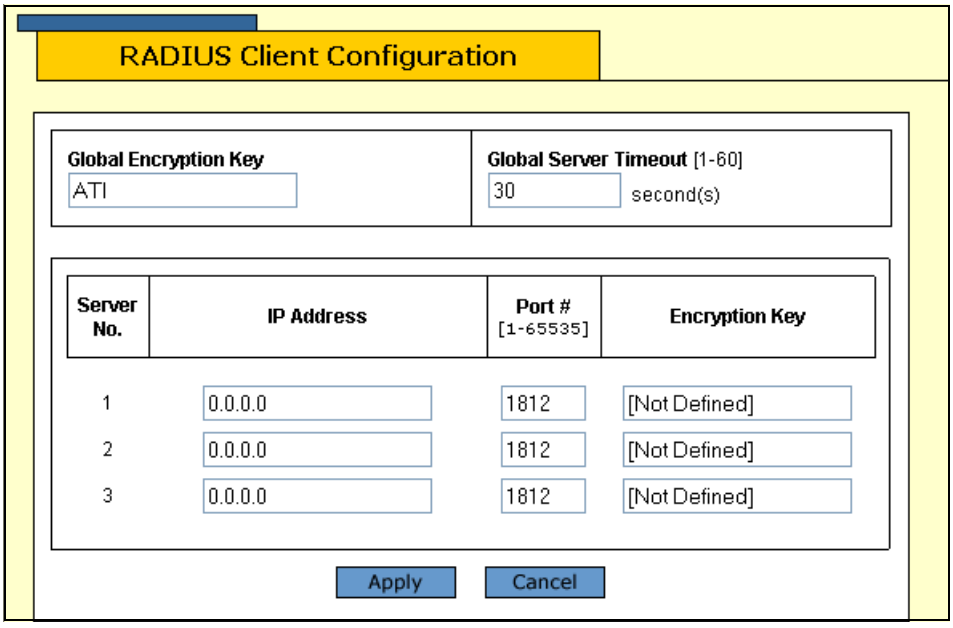

Figure 181. RADIUS Client Configuration Page

4. Configure the following parameters as necessary.

   Global Encryption Key
   If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

   Global Server Timeout
   This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server

cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and **Encryption Key**
Use these fields to specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to a maximum of three servers. You can leave the encryption field blank if you entered the server's key in the Global Secret field.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the RADIUS Settings

To display the RADIUS settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 179 on page 436.

2. Select the **Mgmt. Protocols** option.

   The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 179 on page 436.

   The upper part of the page shows if server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view either the settings for the current authentication method.

3. In the lower portion of the page, click **RADIUS Settings**.

4. Click **View**.

   The RADIUS Client Configuration page is shown in Figure 180.

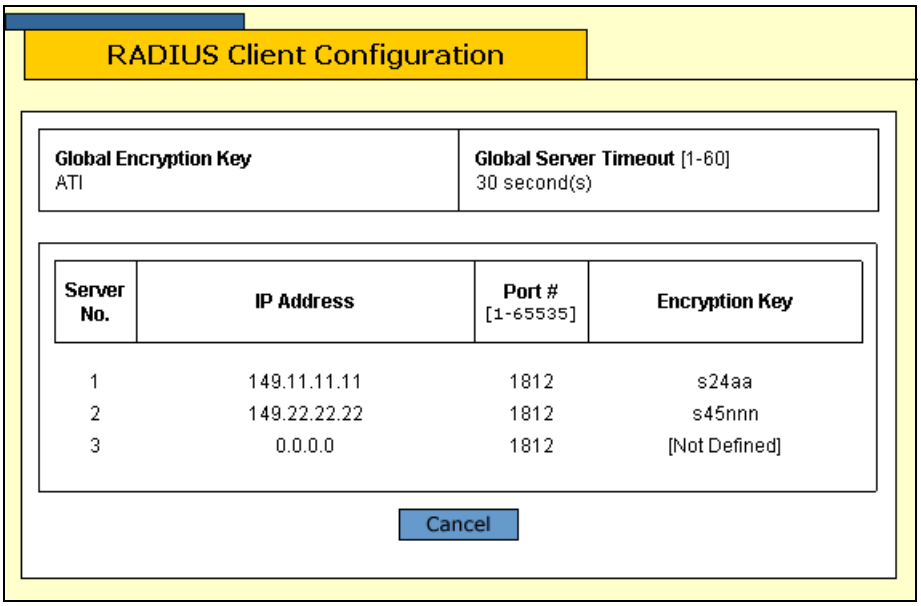

Figure 182. RADIUS Client Configuration Page

The upper portion of the page displays the following information:

Global Encryption Key
The global encryption secret.

Global Server Timeout
The maximum amount of time the switch waits for a response from a RADIUS server before assuming the server cannot respond.

The lower portion of the page displays a table that contains the following columns of information:

Server #
The server number, one of three.

IP Address
IP address of the RADIUS server.

Port
Port of the RADIUS server.

Encryption Key
Encryption key for that server. This parameter is blank if all the RADIUS servers have the same encryption secret.

Chapter 29

Management Access Control List

A management access control list (ACL) allows you to restrict Telnet and web browser management access to the switch. The sections in this chapter include:

- ❒ “Enabling or Disabling the Management ACL” on page 444
- ❒ “Creating an ACE” on page 446
- ❒ “Deleting an ACE” on page 448
- ❒ “Displaying the Management Access Control List” on page 449

Note
For background information about management access control lists, refer to Chapter 37, “Management Access Control List,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Enabling or Disabling the Management ACL

This procedure enables and disables the management ACL. When enabled, only those management stations specified by the access control entries in the ACL are allowed to manage the switch remotely using the Telnet application protocol or a web browser. When the feature is disabled, any remote management workstation can access the switch.

Note
Do not activate the management ACL until you have specified the access control entries (ACEs). Otherwise, the switch will discard all remote management packets, making it impossible for you to remotely manage the unit from a Telnet or web browser management session. For instructions on how to add ACEs, refer to “Creating an ACE” on page 446.

To enable or disable the management ACL, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Security** option.

   The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 183.

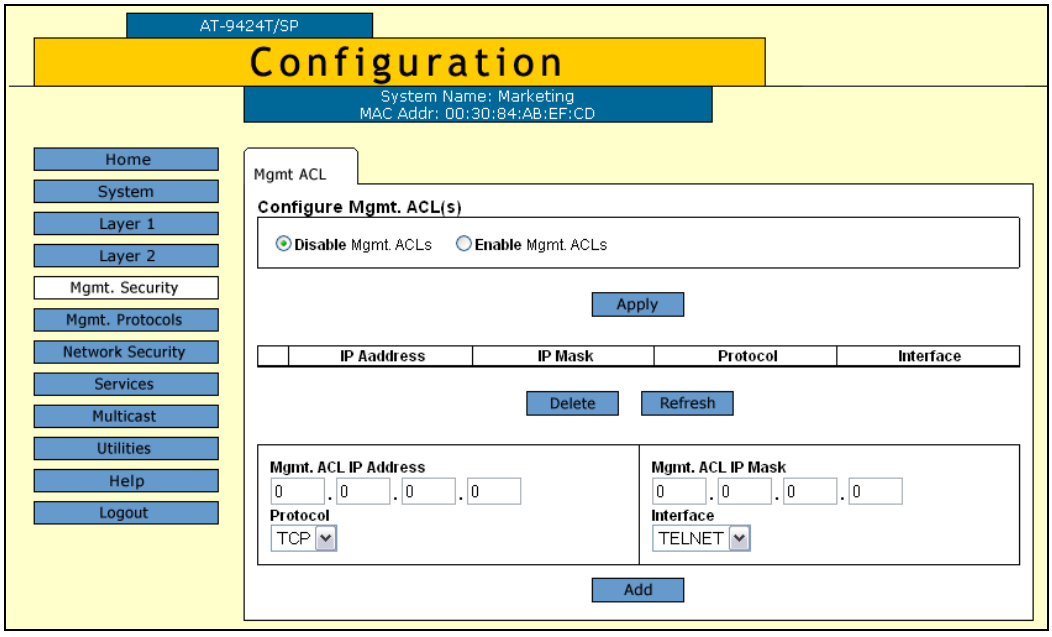

Figure 183. Mgmt. ACL Tab (Configuration)

The middle section of the tab lists the existing ACEs on the switch. The bottom portion is used to add and delete entries. For instructions, refer to "Creating an ACE" on page 446 and "Deleting an ACE" on page 448,

3. Click either **Enable MGMT**. **ACL** or **Disable MGMT**. **ACL**. The default setting is disabled.

4. Click **Apply**.

   A change to the status of the management ACL is immediately activated on the switch.

   Note
   If you activate the feature before entering an access control entry that specifies your management workstation, either by its IP address or subnet, your web browser management session will end and you will not be able to reestablish it.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Creating an ACE

To add a new ACE to the management ACL, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Security** option.

   The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 183 on page 444.

   Any ACEs already existing in the management ACL are listed in the middle section of the tab.

3. To add a new ACE, configure the following parameters in the Mgmt. ACT tab:

   Mgmt. ACL IP Address
   Enter the IP address of a management workstation that you want to be able to manage the switch (for example, 149.11.11.11). Alternatively, you can specify a subnet. You must enter an IP address. If you enter an IP address of a specific management node, then that node will be permitted remote management access to the switch. If you enter a subnet, any management node in the subnet will be permitted remote management access to the switch.

   Protocol
   Specify the protocol of the management packets. There is only one selection, TCP.

   Mgmt. ACL IP Mask
   Enter a mask that indicates the parts of the IP address the switch should filter on. A binary “1” indicates the switch should filter on the corresponding bit of the address, while a “0” indicates that it should not. If you are filtering on a specific IP address, use the mask 255.255.255.255. If you are filtering on a subnet, the mask will depend on the address. For example, to allow all management workstations in the subnet 149.11.11.0 to manage the switch, you would enter the mask 255.255.255.0.

   Interface
   Specify the interface you want the management station to be able to use when managing the switch. The options are:

   Telnet - Allows Telnet management packets.

   Web - Allows web browser management packets.

All - Allows both Telnet and web browser management packets.

4. Click **Add**.

   The management ACL is added to the table displayed in the middle section of the tab.

5. If desired, repeat Steps 3 and 4 to add more ACEs to the Management ACL.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an ACE

To delete an ACE from the management ACL, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 38.

2. From the Configuration menu, select the **Mgmt. Security** option.

   The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 183 on page 444.

3. Select the ACE you want to delete from the table in the middle section of the tab and click **Delete**.

   The ACE is deleted from the list. To see the new list, click **Refresh**.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Management Access Control List

To display the management access control list and its access control entries, perform the following procedure:

1. From the home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 42.

2. From the Monitoring menu, select the **Mgmt. Security** option.

   The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 184.

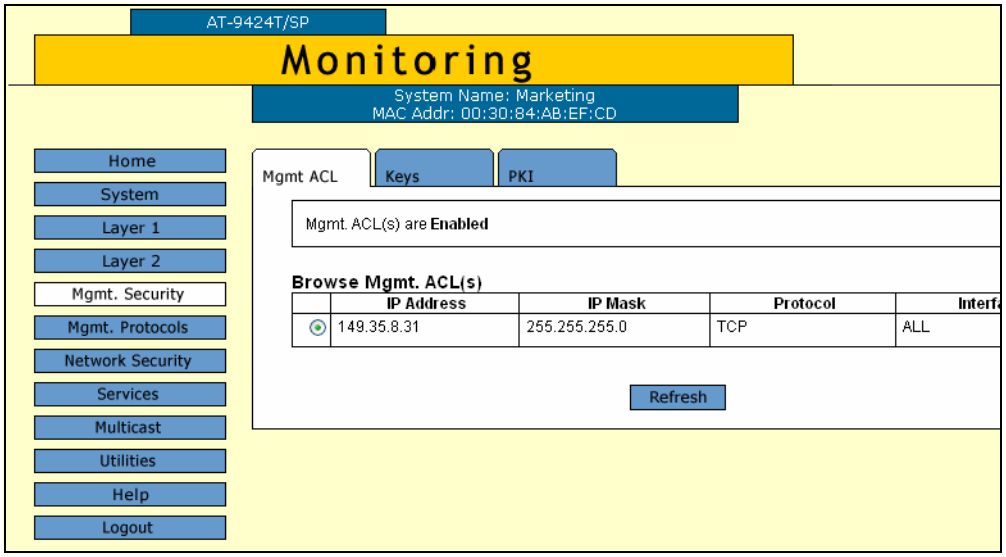

Figure 184. Mgmt. ACL Tab (Monitoring)

The Mgmt. ACL tab contains two sections of information. The top section shows if the management ACL feature is enabled or disabled.

The bottom section displays a table that lists the existing ACEs with the following columns of information:

IP Address
The IP address of a management station or subnet.

IP Mask
A mask that indicates the parts of the IP address the switch should filter on.

Protocol
The protocol for the management packets.

Interface
The interface the management station uses when managing the switch.

Index

Numerics

802.1x Port-based Network Access Control
- access role, configuring 398
- authenticator port, configuring 401
- configuring 398
- disabling 400
- enabling 400
- port parameters, displaying 408
- port role, configuring 398
- port status, displaying 407
- supplicant port, configuring 405

A

active boot configuration file, setting 130
administrator name
- configuring 39

aging time
- changing 101

app (applicant state machine) 368
associations, VLANs to MSTI IDs 330
AT-S63 software
- resetting to factory defaults 52

auth period 406
authentication protocols, enabling or disabling 432
automatic port security level 393
autonegotiation, configuring 80

B

back pressure
- configuring 82

boot configuration file 130
Boot Protocol (BootP)
- activating 41

bridge forwarding delay
- Multiple Spanning Tree Protocol (MSTP) 324
- Rapid Spanning Tree Protocol (RSTP) 314
- Spanning Tree Protocol (STP) 306

bridge hello time
- Multiple Spanning Tree Protocol (MSTP) 324
- Rapid Spanning Tree Protocol (RSTP) 314
- Spanning Tree Protocol (STP) 306

bridge identifier
- Rapid Spanning Tree Protocol (RSTP) 314
- Spanning Tree Protocol (STP) 307

bridge max age
- Multiple Spanning Tree Protocol (MSTP) 324
- Rapid Spanning Tree Protocol (RSTP) 314
- Spanning Tree Protocol (STP) 306

bridge priority
- Rapid Spanning Tree Protocol (RSTP) 313
- Spanning Tree Protocol (STP) 305

bridge protocol data unit (BPDU) 314
browser tools 31

C

ciphers available parameter 429
CIST priority parameter 325
Class of Service (CoS)
- configuring 182
- mapping to egress queues 184
- schedule, displaying 190
- scheduling, configuring 186
- settings, displaying 188

Common and Internal Spanning Tree (CIST), configuring 325
community name
- SNMPv1 and SNMPv2c 67
- SNMPv3 protocol 283, 286

CoS. *See* Class of Service (CoS)

D

data compression parameter 429
daylight savings time (DST) 49
Denial of Service (DoS) defense
- configuring 214
- enabling or disabling 216
- mirror port 216
- settings, displaying 217

document conventions 19
DoS. *See* Denial of Service (DoS) Defense
duplex mode
- configuring 80

Dynamic Host Control Protocol (DHCP)
- activating 41

E

edge port
- Multiple Spanning Tree Protocol (MSTP) 336

encryption keys, displaying 418
enhanced stacking
- changing switches 58
- configuring 56
- setting switch status 56

event log
- clearing 150
- disabling 142
- displaying 144

enabling 142
saving to a file 150
severity codes 149
software module list 147

F

factory defaults
resetting switch 52
flash memory, displaying files in 126
flow control
configuring 82
flow group
configuring 192
deleting 195
displaying 195
modifying 194
force version
Multiple Spanning Tree Protocol (MSTP) 324
Rapid Spanning Tree Protocol (RSTP) 313

G

GARP VLAN Registration Protocol (GVRP)
configuration, displaying 363
configuring 360
counters, displaying 370
database, displaying 366
disabling 362
enabling 362
GIP connected ports ring, displaying 373
GVRP state machine, displaying 367
port configuration, displaying 365
gateway address
configuring 40
displaying 43
global encryption key
configuring 438, 441
global secret
configuring 434, 437
global server timeout
configuring 434, 437
GVRP. *See* GARP VLAN Registration Protocol (GVRP)

H

hardware information 42
held period 406
hello time
Rapid Spanning Tree Protocol (RSTP) 314
Spanning Tree Protocol (STP) 306
host key ID parameter 427
host nodes, displaying 223
host/router timeout interval
configuring 221, 224

I

IGMP. *See* Internet Group Management Protocol (IGMP) Snooping
ingress packet threshold 83
Internet Group Management Protocol (IGMP) snooping
configuring 220
disabling 220, 223
displaying 223
enabling 220, 223
Internet Protocol (IP) address
configuring 40
intrusion action 393
intrusion action (port)
configuring 396

L

limited port security level 393
locked port security level 393
login timeout parameter 427

M

MAC address aging time
changing 101
MAC address table, displaying 98
MAC addresses
adding 94
deleting dynamic 97
deleting multicast 96
displaying 98
MACs available parameter 429
management access control list
disabling 444
enabling 444
management access levels 44
management VLAN ID
configuring 357
management VLAN, specifying 357
manager access 44
manager password
configuring 44
master switch
assigning 56
defined 56
returning to 61
max age
Rapid Spanning Tree Protocol (RSTP) 314
Spanning Tree Protocol (STP) 306
max hops, Multiple Spanning Tree Protocol (MSTP) 324
max requests 403
max start 406
maximum multicast groups
configuring 221
displaying 224
MDI/MDIX mode 81
MSTI ID
creating 326
deleting 327
modifying 328
MSTI ID association to a VLAN
adding 330
modifying 331
MSTI. *See* Multiple Spanning Tree Instance (MSTI)
MSTP. *See* Multiple Spanning Tree Protocol (MSTP)
multicast groups, maximum
configuring 221

displaying 224
multicast host topology
configuring 220
displaying 223
multicast MAC address
adding 94
deleting 96
displaying 98
multicast router ports
configuring 221, 224
multicast routers, displaying 226
Multiple Spanning Tree Instance (MSTI)
associating to VLANs 330
disassociating from VLANs 330
modifying association to VLANs 331
MSTI ID
creating 326
deleting 327
modifying 328
removing a VLAN association 330
Multiple Spanning Tree Protocol (MSTP)
associating VLANs to MSTI IDs 330
bridge forwarding delay 324
bridge hello time 324
bridge max age 324
bridge settings, configuring 322
configuration name 324
configuring 322
connecting to VLANs 330
disabling 320
edge port 336
enabling 320
force version 324
max hops 324
MSTI ID
creating 326
deleting 327
modifying 328
parameters, configuring 322
point-to-point port 335
port external path cost 335
port internal path cost 334
port parameters
configuring 333
displaying 337
port priority 334
port settings, displaying 340
port status, displaying 340
resetting to defaults 342

O

operator access 44
operator password
configuring 44

P

password
changing 44
default 29
piggyback mode 404
pinging 50
PKI certificates
displaying 420
PKI certificates, displaying 420
PKI. *See* Public Key Infrastructure (PKI)
point-to-point port
Multiple Spanning Tree Protocol (MSTP) 335
Rapid Spanning Tree Protocol (RSTP) 315
policy
configuring 206
deleting 210
displaying 210
modifying 208
port
configuring parameters, basic 78
disabling 79
enabling 79
link status 86
resetting to defaults 92
statistics, displaying 89
status
displaying 85
port control
802.1x port-based access control 402
force-authorized 403
force-unauthorized 403
port cost
Multiple Spanning Tree Protocol (MSTP) 334
Rapid Spanning Tree Protocol (RSTP) 315
Spanning Tree Protocol (STP) 308
port mirror
creating 114
deleting 119
disabling 118
displaying 120
modifying 117
port parameters, configuring
basic 78
Multiple Spanning Tree Protocol (MSTP) 322
Rapid Spanning Tree Protocol (RSTP) 312
Spanning Tree Protocol (STP) 304
port participating parameter 394
port priority
Multiple Spanning Tree Protocol (MSTP) 334
Rapid Spanning Tree Protocol (RSTP) 315
Spanning Tree Protocol (STP) 307
port security
displaying 395
intrusion action 396
port security levels, MAC 393
port speed
configuring 80
port trunk
creating 104
deleting 109
displaying 110
modifying 107

port-based access control. *See* 802.1x Port-based Network Access Control
port-based VLAN
    creating 346
    deleting 352, 385
    displaying 355, 386
    modifying 350
protected ports VLAN
    creating 376
    deleting 385
    displaying 386
    modifying 381
Public Key Infrastructure (PKI)
    settings, displaying 420

Q

QoS. *See* Quality of Service (QoS)
Quality of Service (QoS)
    See also traffic class, flow group, and policy 191
quiet period, configuring 403

R

RADIUS
    configuring 438
    disabling 432
    displaying settings 440
    enabling 432
    server timeout 441
RADIUS accounting
    configuring 411
    settings, displaying 412
RADIUS server
    encryption secret 439
    encryption secret, configuring 435
    IP address, configuring 439
Rapid Spanning Tree Protocol (RSTP)
    bridge forwarding delay 314
    bridge hello time 314
    bridge identifier 314
    bridge max age 314
    bridge priority 313
    bridge settings, configuring 312
    disabling 302, 320
    edge port, configuring 315
    enabling 302, 320
    force version 313
    point-to-point port, configuring 315
    port cost 315
    port priority 315
    port settings, displaying 316, 340
    resetting to defaults 316
rate limit, setting 83
reauth period, configuring 403
reg (registrar state machine) parameter 369
RSTP. *See* Rapid Spanning Tree Protocol (RSTP)

S

Secure Shell (SSH) protocol
    configuring 426
    displaying settings 428
Secure Sockets Layer (SSL)
    displaying settings 423
secured port security level 393
server authentication UDP port
    configuring 439
server key ID parameter 427
server timeout, configuring 404
session cache timeout
    configuring 423
Simple Network Time Protocol (SNTP)
    configuring 47
    servers 47
slave switch
    assigning 56
    defined 56
SNMP management
    disabling 64
    enabling 64
SNMPv1 and SNMPv2c community
    creating 66
    deleting 72
    displaying 73
    modifying 69
SNMPv3 Access Table entry
    creating 250
    deleting 253
    displaying 291
    modifying 254
SNMPv3 community name, modifying 286
SNMPv3 Community Table entry
    creating 282
    deleting 285
    displaying 296
    modifying 285
SNMPv3 Notify Table entry
    creating 263
    deleting 265
    displaying 293
    modifying 266
SNMPv3 SecurityToGroup Table entry
    creating 257
    deleting 260
    displaying 292
    modifying 260
SNMPv3 Target Address Table entry
    creating 268
    deleting 271
    displaying 294
    modifying 272
SNMPv3 Target Parameters Table entry
    creating 275
    deleting 278
    displaying 295
    modifying 279

SNMPv3 User Table entry
creating 236
deleting 239
displaying 288
modifying 240
SNMPv3 View Table entry
creating 244
deleting 247
displaying 290
modifying 247
SNTP. See Simple Network Time Protocol (SNTP)
software information 42
Spanning Tree Protocol (RSTP)
parameters, displaying 308
Spanning Tree Protocol (STP)
bridge forwarding delay 306
bridge hello time 306
bridge identifier 307
bridge max age 306
bridge parameters, configuring 304
bridge priority 305
disabling 302, 320
enabling 302, 320
parameters, displaying 308
port cost 308
port priority 307
port settings, displaying 340
resetting to defaults 311
SSH. *See* Secure Shell (SSH)
SSL. *See* Secure Sockets Layer (SSL)
static MAC address
adding 94
deleting 96
static unicast MAC address, displaying 98
STP ID 373
STP. *See* Spanning Tree Protocol (STP)
subnet mask
configuring 40
supplicant port, start period 406
supplicant timeout 403
switch
hardware information 42
software information 42
switch name, configuring 38
switch, rebooting 46
system date
setting 47
system file
downloading 134
uploading 139
system name
configuring 39
system time
setting 47

T

TACACS+
configuring 434
disabling 432
displaying settings 436
enabling 432
server timeout
configuring 438
tagged VLAN
creating 346
deleting 352, 385
displaying 355, 386
modifying 350
threshold 394
traffic class
configuring 198
deleting 202
displaying 202
modifying 200
tx period, configuring 403

U

unavailable status, defined 56
uplink port
configuring 354
displaying 356
user name
configuring 406
default 29
user password, configuring 406

V

versions supported (SSH) parameter 428
virtual LAN (VLAN)
associating to MSTI IDs 330
creating 346
deleting 352, 385
displaying 355, 386
mode, selecting 353
modifying 350
VLAN identifier (VID)
configuring 376
VLAN name
configuring 376
VLAN type
port-based or tagged VLAN 348

W

web browser management session
quitting 33
starting 28